内 容 简 介

本书应用伽罗瓦理论清晰透彻地论述了两个古典难题的解决方法，即寻找代数方程的求根公式和限用圆规直尺作图（如三等分任意角、把立方体体积加倍、化圆为正方形以及作正多边形等），并借此由浅入深地向读者介绍了一些抽象代数的基本知识和研究方法。本书可作为理工科学生和其他数学爱好者学习抽象代数的普及读物，也可供大中学校数学教师阅读参考。

写 在 前 面

近几年来，仍然有人宣布已成功地用圆规直尺将任意角三等分。他们把稿件投寄有关部门，但一般都得不到答复。事实上，这一问题早已被证明是不可能的。“不予审阅，妥为保存”，这已成为处理这种特殊稿件的专门方法。据说，法国科学院曾作出决议，凡是关于三等分角、倍立方、化圆为方和永动机的文章一律不予审阅。作者愿把这本小册子奉献给读者，也算是一个肤浅的答复和解释吧！书中所提到的五大难题，曾折磨了人们二千多年，致使有些了不起的数学家也曾为之冥思苦想，虚掷光阴，直到十九世纪伽罗瓦引入了置换群，创立了抽象代数学，才透彻地解决了这些难题。作者恳切希望至今仍迷恋于这些已有定论之难题的人们，不要再浪费时间和精力了。当然，有些人相信这些问题已有结论，但他们“只知其然，不知其所以然”，总希望能看到一些普及读物，以便了解这些问题是如何解决的。更进一步，近一个世纪以来，抽象代数学已成为一门重要学科，它的应用已遍及各个数学分支，甚至扩及其他科学领域。然而，不少大学生、青年教师和科技工作者却没有机会系统地学习这门学科。因此，作者希望通过对伽罗瓦理论的介绍，普及某些最基本的抽象代数学知识，让读者了解抽象代数学处理问题和解决问题的方法。

抽象代数，顾名思义是抽象的代数，而这也正是使某些人“望而却步”的原因之一。的确，抽象代数可谓是抽象概念的宝塔，逻辑推理的楷模。应该说，抽象是个好法宝，经

过抽象往往更能看清事物的本质和各个事物相互之间的联系。事实上，任何有生命力的抽象概念都有广泛的实际背景，决不是凭空臆造出来的空中楼阁。为了尽量减轻阅读难度，我们将比较自然地引入一些必要而又基本的概念，采取尽可能简单的途径证明一些结论，並力求讲得通俗易懂些，至于逻辑推理，只要习惯了，也就不难了。

本书从初等代数和初等几何中的古典难题讲起，由浅入深地介绍抽象代数、特别是伽罗瓦理论的基本知识，任何受过一定数学训练的读者都能读懂本书。

全书共分四章，在第一章中介绍有关历史，所引用的史料，由于出处不一，仅供参考。第二章介绍有关的群论知识。伽罗瓦理论的核心内容将在第三章中讨论。第四章是它的一些应用，详细地叙述了五大难题是如何解决的。

在本书的编写过程中，周仲良同志和顾海燕同志曾认真地阅读了全书，並提出了不少修改意见，作者在此对他们表示衷心的感谢。由于作者学识浅，水平低，在本书中难免有不当之处，望读者批评指正。

徐诚浩

一九八四年国庆

目　录

第一章 历 史 概 况

§1 高次代数方程的求根公式

根据古埃及的草片文书①记载，早在公元前1700年左右，人们就发现，当 $a\neq 0$ 时，$ax=b$ 有根 $x=b/a$。随着岁月的流逝，数学发展了。到了公元前几世纪，巴比伦(现在伊拉克的一部份)人实际上已经使用过配方法得知 $ax^2+bx+c=0$ (当 $a\neq 0$ 时)有根

$$x=\frac{1}{2a}\left(-b\pm\sqrt{b^2-4ac}\right)。$$

当时，人们只承认现在称之为正实数的根才是根。零、负数、无理数和复数的概念和理论迟至十六世纪到十八世纪才得到承认并逐步完善。根据巴比伦的泥板文书①记载，当时已解决了如下二次方程问题：求出某数 x，使其与其倒数之和等于给定数 b，即 $x+1/x=b$。得出的解答是

$$x=\frac{b}{2}\pm\sqrt{\left(\frac{b}{2}\right)^2-1},$$

这就促使人们进一步思考，是否对于任意次数的方程都能找

① 草片是一种把木髓紧压后切成的薄片，用墨水写上象形数字就成了草片文书。下述的泥板文书则是在胶泥尚软时刻上楔形数字然后晒干得到的文书。

到这种求根公式？寻找三次方程的求根公式，经历了二千多年的漫长岁月，直到十六世纪欧洲文艺复兴时期，才由几位意大利数学家找到，这就是通常所说的卡丹(J. Cardan，1501～1576)公式。其原始的想法是：在

$$x^3+ax^2+bx+c=0$$

中作变量代换 $x=y-a/3$ 后化为

$$y^3+py=q, \tag{1}$$

它不再含有平方项了。设 $y=\sqrt[3]{m}-\sqrt[3]{n}$，这里 m 和 n 是两个待定的数，则有

$$y^3=m-n-3\cdot\sqrt[3]{mn}\,y=q-py。$$

如果取 m、n 满足

$$m-n=q,\ \sqrt[3]{mn}=\frac{p}{3},$$

则对应的 y 值必满足(1)式。另一方面，由

$$(m+n)^2=(m-n)^2+4mn=q^2+\frac{4}{27}p^3,$$

可得

$$m+n=\sqrt{q^2+\frac{4}{27}p^3}.$$

所以，当取

$$m=\frac{1}{2}q+\sqrt{\frac{1}{4}q^2+\frac{1}{27}p^3},\quad n=-\frac{1}{2}q+\sqrt{\frac{1}{4}q^2+\frac{1}{27}p^3}$$

时，并令 $\alpha=\sqrt[3]{m}$，$\beta=\sqrt[3]{n}$，就得原三次方程的一个根

$$x_1=\alpha-\beta-a/3,$$

它的另两个根是

$$x_2=\omega\alpha-\omega^2\beta-a/3,$$

$$x_3=\omega^2\alpha-\omega\beta-a/3,$$

这里 $\omega=(-1+\sqrt{3}i)/2$,

$\omega^2=(-1-\sqrt{3}i)/2$　　(其中 $i=\sqrt{-1}$)

是 $x^3-1=0$ 的两个不是 1 的根。

关于卡丹，历史上评价不一，可谓是毁誉参半。在他晚年所著《我的生平》一书中，他对自己既有褒扬之词，但也不乏贬抑之语。卡丹既是闻名全欧的医生，又是颇为人知的数学教授。他既对数学、物理学作出过不少贡献，又精通赌博和占星术，而且还曾写过有关赌博的专著。他曾因犯有给耶稣基督算命的异端罪行而被捕入狱，然而教皇却也将他奉为座上宾，请他当占星术士。在三次方程求根公式的发明过程中，卡丹还有一段不甚光彩的轶事。这就要从四百多年前的一场数学竞赛谈起了。竞赛的内容是求解三次方程。竞赛的一方是菲俄（A.M.Fior，十六世纪前半叶），他是意大利波洛那（Bologna）数学学会会长费尔洛（S.d.Ferro，1465～1526）的学生。另一方是威尼斯的数学教授方丹诺（N.Fontana，1499？～1557）。不过他的这个真名鲜为人知，留传于后世的倒是他的绰号——塔尔塔里亚（Tartaglia），意思是“口吃者”。在他幼年时，正值意法战争。其父被法国兵杀害，他的头部和上、下颚被法国兵用马刀砍成重伤。后来，他的母亲在尸骸堆中把他找到，用舌舔其伤口，居然得救，但已得了口吃之疾。他自学拉丁文、希腊文，酷爱数学。与费尔洛一样，对求解三次方程很有研究。在 1530 年，塔尔塔里亚曾解决了另一个挑战者科拉（Colla）提出的以下两个三次方程求解问

题：$x^3+3x^2=5$，$x^3+6x^2+8x=1000$。这引起菲俄的不服，定于1535年2月22日在米兰大教堂公开竞赛，双方各出三十个三次方程。结果，塔尔塔里亚在两小时内解完，而菲俄却交了白卷。1541年，塔尔塔里亚得到了三次方程的一般解法，准备在译完欧几里得和阿基米德的著作后，自己写一本书公开他的解法。此时，卡丹出场了。他再三乞求塔尔塔里亚把解法告诉他，并发誓保守秘密。塔尔塔里亚给他一首语句晦涩的诗。这首诗写得很蹩脚，但的确把解法的每一步骤都写进去了。他本人也说："本诗有无佳句，对此我不介意。为记这一规则，此诗堪作工具。"(另一种说法是，卡丹是在塔尔塔里亚的朋友处答应保密后套出了这首诗的）卡丹在得到这一切以后，却背信弃义，于1545年把这一解法发表在《大术》这本书中，并断定塔尔塔里亚的方法就是费尔洛的方法，他是在与菲俄竞赛时得知的。这引起塔尔塔里亚的极大愤怒，并向卡丹宣战。双方各出31题，限定15天交卷。卡丹派他的学生费尔拉里(L.Ferrari,1522～1565)应战。结果，塔尔塔里亚在七天之内解出大部份题目，而费尔拉里五个月后才交卷，仅解对了一题。塔尔塔里亚本想完成一部包含他的新算法在内的巨著，可惜壮志未酬就与世长辞了！在三次方程的求解问题解决后不久，费尔拉里又得到了四次方程的求解方法。其主要思路是：对于四次方程

$$x^4+ax^3+bx^2+cx+d=0 \qquad (2)$$

引入参数t，经过配方化为

$$\left(x^2+\frac{1}{2}ax+\frac{1}{2}t\right)^2$$

$$=\left(\frac{1}{4}a^2-b+t\right)x^2+\left(\frac{1}{2}at-c\right)x+\left(\frac{1}{4}t^2-d\right)。\qquad (3)$$

容易验证(2)与(3)式是一样的.为了保证(3)式右边是完全平方,可令它的判别式为 0:

$$\left(\frac{1}{2}at-c\right)^2-4\left(\frac{1}{4}a^2-b+t\right)\left(\frac{1}{4}t^2-d\right)=0,$$

即选择 t 是三次方程

$$t^3-bt^2+(ac-4d)t-a^2d+4bd-c^2=0$$

的任一根。把这个根作为(3)中的 t 值就有

$$\left(x^2+\frac{1}{2}ax+\frac{1}{2}t\right)^2=\left(\sqrt{\frac{1}{4}a^2-b+t}\ x+\sqrt{\frac{1}{4}t^2-d}\right)^2.$$

把右边移到左边并分解因式得到两个二次方程

$$x^2+\left(\frac{1}{2}a-\sqrt{\frac{1}{4}a^2-b+t}\right)x+\frac{1}{2}t-\sqrt{\frac{1}{4}t^2-d}=0,$$

$$x^2+\left(\frac{1}{2}a+\sqrt{\frac{1}{4}a^2-b+t}\right)x+\frac{1}{2}t+\sqrt{\frac{1}{4}t^2-d}=0.$$

这样，就把求四次方程的根化为求一个三次方程和两个二次方程的根，因此，可以认为四次方程求解问题也解决了。既然有了这个突破，数学家们就以极大兴趣和自信致力于寻找五次方程的求解方法。他们发现,对次数不超过四的方程,都能得到根的计算公式，每个根都可用原方程的系数经过加减乘除和开方运算表出。我们把这件事简称为**可用根号求解**。于是人们就断言：对五次方程来说，也一定存在这种求根公式.关于这一点，当时的一些著名数学家，如欧拉(L.Euler, 1707～1783)、范达蒙(Van der monde,1735～1796)、拉格朗日(J.L.Lagrange,1736～1813)、鲁菲尼(P.Ruffini, 1765～1822)和高斯 (K.F.Gauss, 1777～1855) 等都曾深信不疑,

因而都曾尽力寻找，但都以失败告终。

首先怀疑这种求根公式存在性的是拉格朗日。他透彻地分析了前人所得的次数低于五的代数方程的求解方法，发现都可作适当变量代换化为求解某些次数较低的辅助方程（它们被后人称为拉格朗日预解式），然而，对于五次方程，按这种方法得到的辅助方程的次数却升至六次，于是此路不通！1771 年，拉格朗日发表长篇论文《关于方程的代数解法的思考》提出了这个怀疑。到了 1813 年，他的弟子，意大利的内科医生鲁菲尼终于证明了拉格朗日所采用的寻找预解式的方法对于五次方程的确是失效的。早在 1801 年，高斯也意识到这个问题也许是不能解决的。可是，包括拉格朗日在内，他们都没有给出"不存在性"的证明。

第一个证明"高于四次的代数方程不能用根号求解"的是挪威青年数学家阿贝尔（N.H.Abel，1802～1829）。他是乡村牧师之子，幼年丧父，家境贫困。在中学时，他就读了拉格朗日和高斯关于方程论的著作，探讨高次方程的求解问题。1824～1826年，他写出《五次方程代数解法不可能存在》一文，但高斯等人表示不理解。阿贝尔在数学方面有很多独创性成就，在当时都未能被重视。由于贫病交迫，1829 年 4 月 6 日死于结核病，年仅 27 岁。在他逝世前不久，曾把一些研究结果告诉了拉让得（A.M.Legendre，1752～1833）。就在他离开人间的第三天，柏林大学给他寄来了教授聘书。

不过，鲁菲尼和阿贝尔的证明毕竟是不很清楚的，甚至还有一些漏洞。阿贝尔并没有给出一个准则用来判定一个具体数字系数的高次代数方程能否用根号求解。作为历史，他们的功绩不容抹煞，但是，若与不久以后出现的伽罗瓦的辉煌成就相比，就大为逊色了！

伽罗瓦 (E.Galois,1811～1832) 是法国青年数学家．他是巴黎附近一个小镇镇长的儿子，15 岁进入巴黎的一个有名的公立中学学习，偏爱数学。后来想进多科工艺学校(即工科大学)，可能是由于口试失误或者主考教授不理解他的思想，竟两次落榜，只得进了一所低等的预备学校．此时，他专攻五次方程代数解法。第一年就写了四篇文章。1828 年，十七岁的伽罗瓦写出《关于五次方程的代数解法问题》等两篇论文送交法国科学院，但被柯西 (A.Cauchy，1789～1875)遗失了。后来，他又把另一篇文章送给傅利叶(J.Fourier，1768～1830)，不久，傅利叶去世，也就不了了之。1831年，伽罗瓦完成了《关于用根式解方程的可解性条件》一文，院士泊松 (S.D.Poisson,1781～1840) 的审查意见却是"完全不能理解"，予以退回。1830 年法国七月革命时，他因批评学校的学监不支持革命而被开除，又因政治罪两次被送进监狱。1832 年 4 月出狱住医院治病．出院当天，在路上遇到两个不速之客，相约于第二天决斗，结果他因受重伤于 5 月 31 日离世，时年不满21岁．在决斗前夜，他深知为女友决斗而死毫无意义，但又不甘示弱．当晚，他精神高度紧张和不安，连呼"我没有时间了！"匆忙之中，他把他的关于方程论的发现草草写成几页说明寄给他的朋友，并附有如下一段话："你可以公开地请求雅科比(C.Jacobi)或者高斯，不是对于这些定理的真实性而是对于其重要性表示意见．将来我希望有一些人会发现把这堆东西注释出来对他们是有益的．"到了 14 年以后的 1846 年，柳维尔 (J.Liouville,1809～1882) 在由他创办的《纯粹数学和应用数学杂志》上发表了伽罗瓦的部份文章。关于伽罗瓦理论的头一个全面而清楚的介绍是在若唐 (C.Jordan，1838～1922)于 1870 年出版的《置换和代数方程专论》一书中给出

的。这样，伽罗瓦超越时代的天才思想才逐渐人所被言理解和承认，至今已成为一门蓬勃发展的学科一抽象代数学。伽罗瓦避开了拉格朗日的难以捉摸的预解式而巧妙地应用置换群这一工具，他不但证明了如下的一般代数方程

$$a_0x^n+a_1x^{n-1}+a_2x^{n-2}+\cdots+a_{n-1}x+a_n=0$$

当 $n\geqslant5$ 时不可能用根号求解（这里系数 a_i 可取任何复数），而且还建立了具体数字系数的代数方程可用根号求解的判别准则，并举出不能用根号求解的数字系数代数方程的实例。这样，他就透彻地解决了这个在长达二百多年的时间中使不少数学家伤透脑筋的问题。不仅如此，伽罗瓦所发现的结果，他的奇特思想和巧妙方法，现已成为全部代数的中心内容。在这一点上说，他作为抽象代数的创始人之一是当之无愧的。他的贡献决不限于解决代数方程根号求解的问题。

§2 圆规直尺作图

在历史上，限用圆规直尺的古希腊四大几何作图难题，一直引起无数数学家和数学爱好者的浓厚兴趣。这里所说的直尺是没有刻度的，并且要求作图必须在有限步完成。为什么非要限用圆规直尺作图呢？希腊人认为，直线和圆弧是构成一切平面几何图形的基本图形，而直尺和圆规则是直线和圆弧的具体化。他们甚至认为只有使用圆规直尺作图才能确保其严密性。到了公元前三世纪的欧几里得时期，创立了以五条公设为基础的欧氏几何，就更加严格限用圆规直尺作图了。现在我们把这四个难题逐一介绍一下。我们约定：凡说到"可

作”，总指限用圆规直尺能在有限步内作出。

(一)**将任意角三等分**．这等价于将任意一段圆弧三等分。中学生学会了用圆规直尺把任意角二等分。那末，自然要问：能否将任意角三等分呢？在历史上的确有过一些三等分角的作图法。早在公元前五世纪，希腊人喜皮亚斯(Hippias，生于公元前 425 年左右)特地为此发明了一种割圆曲线，用它可把任意角三等分．割圆曲线的作法如下：在平面上作 AB

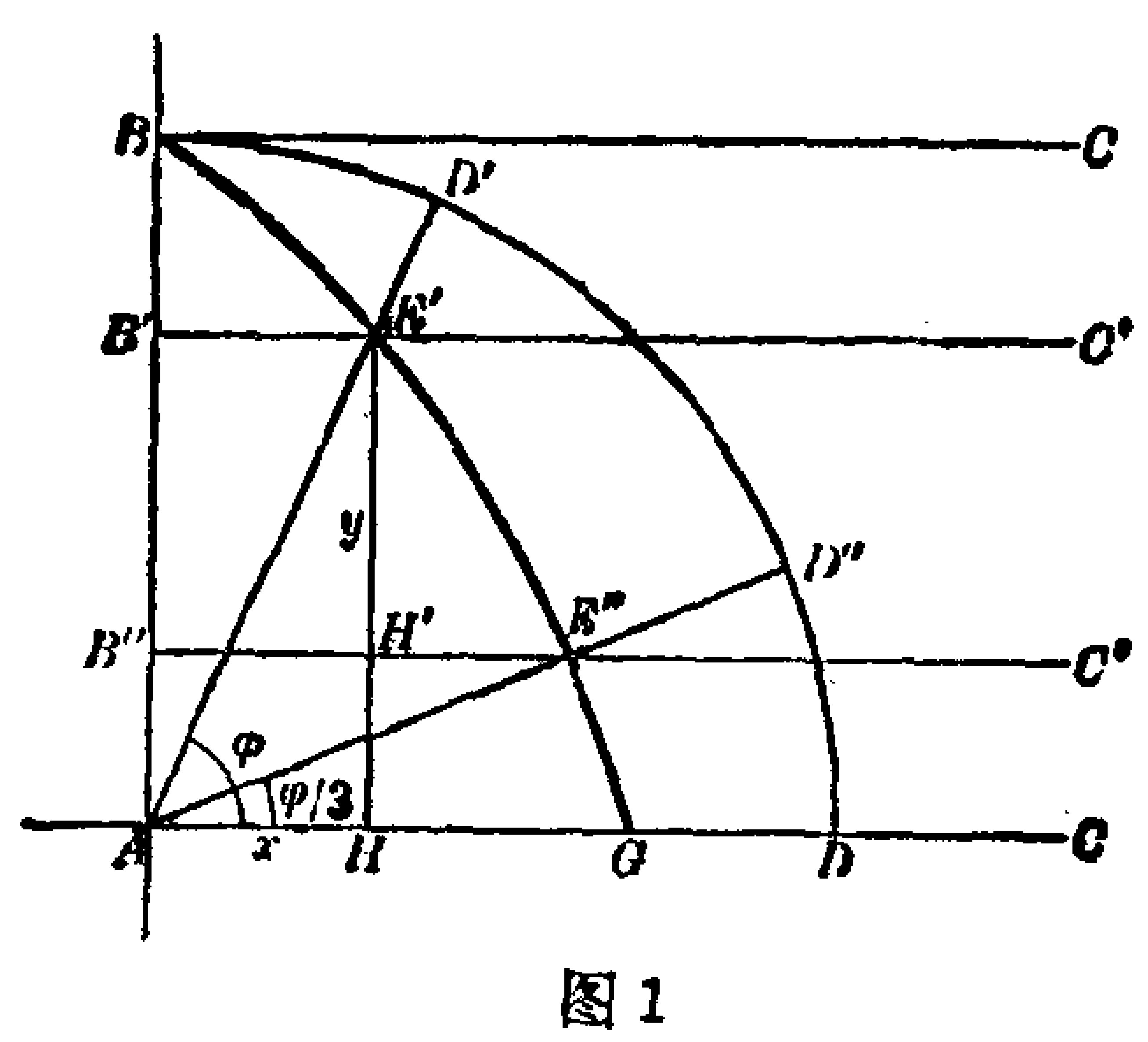


图1

垂直于 AD，且 $|AB|=|AD|$．作 BC 平行于 AD。将 AB 绕 A 点顺时针匀速转到 AD。同时，将 BC 匀速平行下移与 AD 重合。设 AB 转到 AD' 时，BC 移到 $B'C'$。AD' 与 $B'C'$ 交于 E'，则这个 E' 就是割圆曲线上的一般点。如果割圆曲线已经作出，那就可把任意角三等分了．不妨设 $\angle E'AD=\varphi$。作 $E'H$ 垂直于 AD，在 AD 上的垂足是 H。把线段 $E'H$ 三等分(这容易用圆规直尺作出，见第137页)，使 $|H'H|=|E'H|/3$，过 H' 作 $B''C''$ 平行于 AD，交割圆曲线于 E''，注意到割圆曲线是按照两个“匀速”的要求作出的，所以必有

$$\frac{\angle E''AD}{90^\circ}=\frac{|H'H|}{|AB|}=\frac{1}{3}\ \frac{|E'H|}{|AB|}=\frac{1}{3}\ \frac{\angle E'AD}{90^\circ}.$$

于是 $\angle E''AD=\angle E'AD/3=\varphi/3$。可惜的是这种割圆曲线是决不可能只用圆规直尺在有限步内作出的。

到了公元前三世纪，希腊数学大师阿基米德（Archimedes，公元前287-212）曾给出一个非常简单的方法：任给 $\angle AOB=\varphi$，设 F 和 F' 是某直尺的两个端点。用有色笔在此直尺

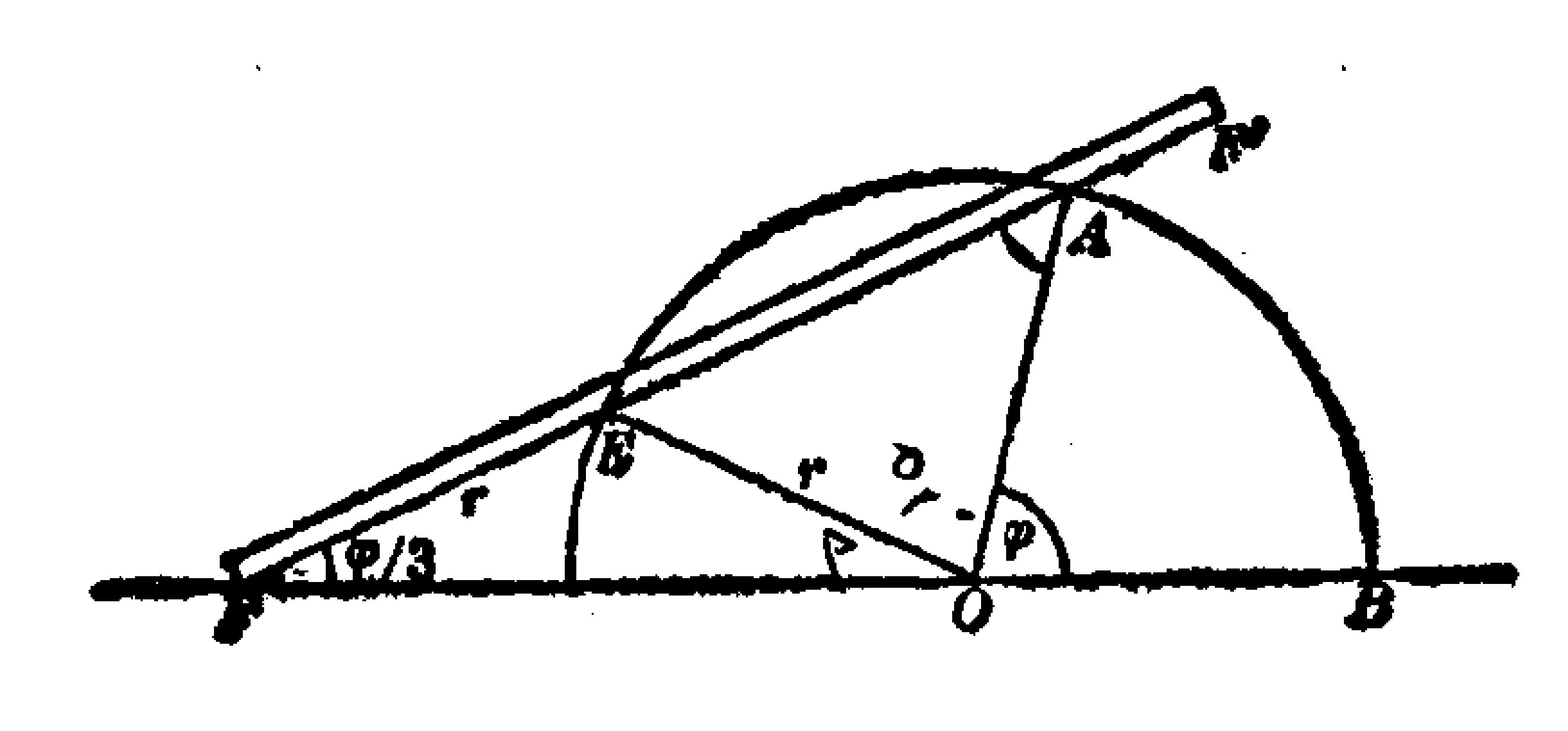


图 2

上任意画上一个点 E。以O为圆心，以 $|EF|=r$ 为半径作半圆，交角 φ 的两边于 A 和 B。现在这样来放置直尺，让 E 在圆周上滑动，F 在 OB 的延长线上滑动，恰使此尺过 A 点，则有

$$\begin{aligned}\varphi=\angle AOB&=\angle AFO+\angle OAE\\&=\angle AFO+\angle OEA=2\angle AFO+\angle EOF\\&=3\angle AFO,\end{aligned}$$

所以 $\angle AFO=\varphi/3$。可惜，在直尺上画上点 E 不符合规尺作图的规定。稍为放松一"点"要求，三等分任意角就可作了！类似这种不易觉察的"想当然"式的漏洞，三等分角者经常会不自觉地产生。当然，阿基米德知道这是犯规的，但苦于无法否定它的可作性。在本书中我们将要证明，的确存在不可以三等分的角，例如 60°。另一方面，只要 n 不能被3整除，角 $\alpha=\pi/n$ 必可三等分。在一百多年前，这个问题已有定论：三等分任意角不可作。企图用圆规直尺把任意角三等分，就

象企图发明永动机一样，是决不会成功的。

(二)**倍立方**。根据历史记载，公元前430年，雅典城流行鼠疫，居民们向地劳斯神殿请求驱除瘟疫，巫神命令他们把现有的立方体祭坛的体积扩大一倍，但仍要保持立方体的形状。于是倍立方问题就产生了。人们去请教柏拉图(Plato)。他说，巫神之意是借此遣责希腊人不重视数学，并对几何学不够尊崇。当然，这些都是传说而已。其实，提出这个问题也是很自然的。因为以任一正方形的对角线为边所得的新正方形，其面积恰是原正方形面积的两倍。这是一个倍平方问题。转而考虑立方体就是倍立方问题了。古希腊的毕达哥拉斯学派的希波克拉提斯(Hippocrates，约公元前460年)早就指出：倍立方问题可归结为求线段 a 与 $2a$ 之间的两个比例中项 x 和 y 的问题，这里 a 是给定立方体的棱长：

$$a:x=x:y=y:2a.$$

事实上，此时有 $x^2=ay$，$y^2=2ax$，$x^4=a^2y^2=2a^3x$。在等式两边约掉 x 后即得

$$x^3=2a^3.$$

于是棱长为 x 的立方体的体积就是棱长为 a 的立方体体积的两倍。但是，这个 x 如何作出呢？后来有人用两把直角尺(称为矩)作出了这个 x。其作法如图3所示。任作两条互相垂直的直线

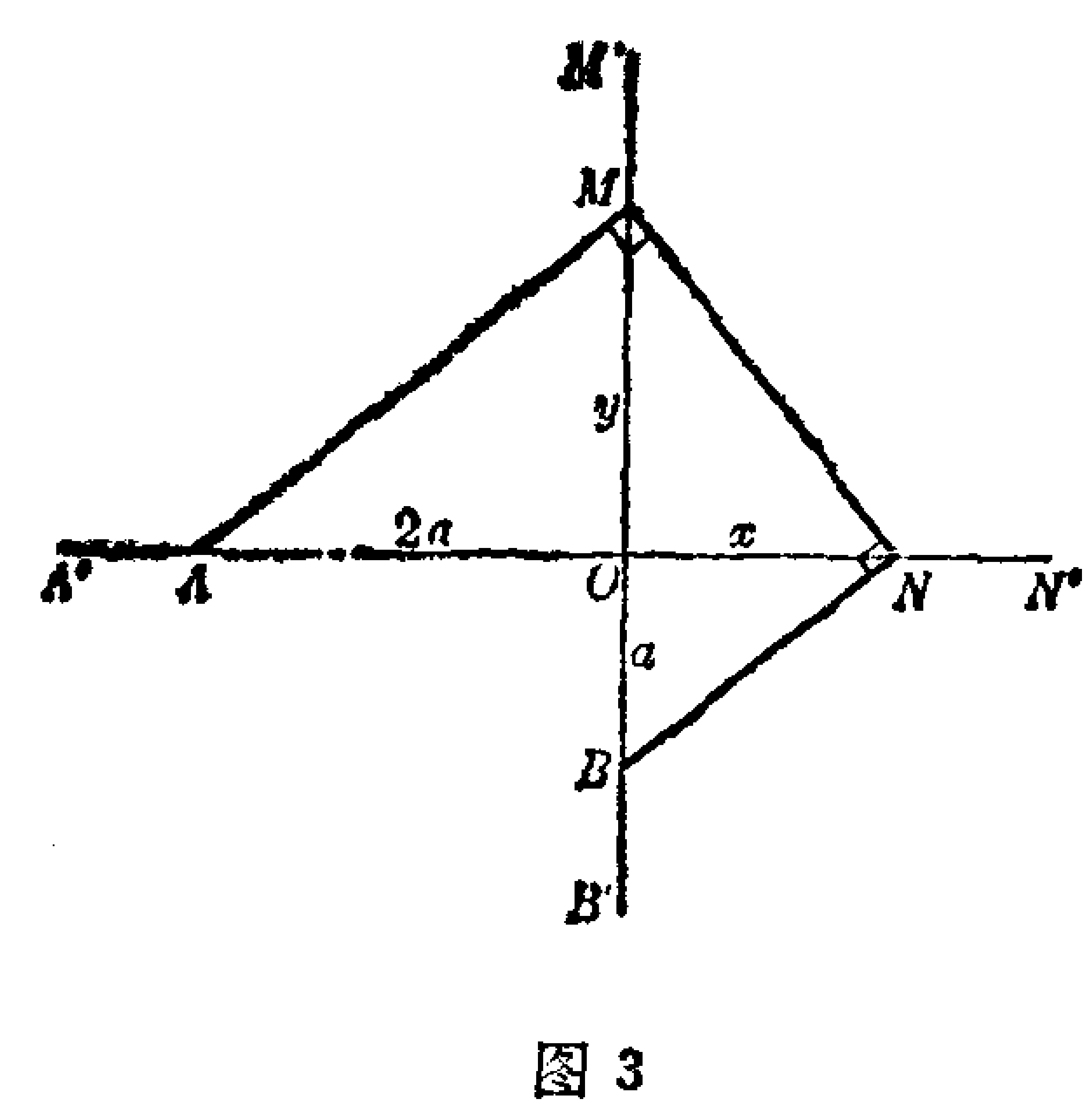


图 3

$M'B'$ 和 $A'N'$，交点为O。截取 $|OB|=a$，$|OA|=2a$。取两把直尺甲和乙。让甲的直角顶在 $M'B''$ 上移动，一条直角边通过 A 点；乙的直角顶在 $A'N'$ 上移动，一条直角边通过 B 点。再如此协调甲和乙的位置，使它们的另一对直角边正好重合，这样就产生了图上的 M 和 N 两点。于是 $|ON|=x$，$|OM|=y$.此 x 即为所求。显然，这不能算是圆规直尺作图。我们将很容易地证明，作出倍立方体的棱长也是圆规直尺无法办到的。

(三)**化圆为方**．求作一正方形使其面积与给定圆的面积相等.这是历史上曾经风靡一时的等积问题(作新图形与原图形的面积相等)的特例。欧洲文艺复兴时期的达·芬奇 (Leonardo de Vinci,1452～1519)曾很巧妙地解决了这个问题：

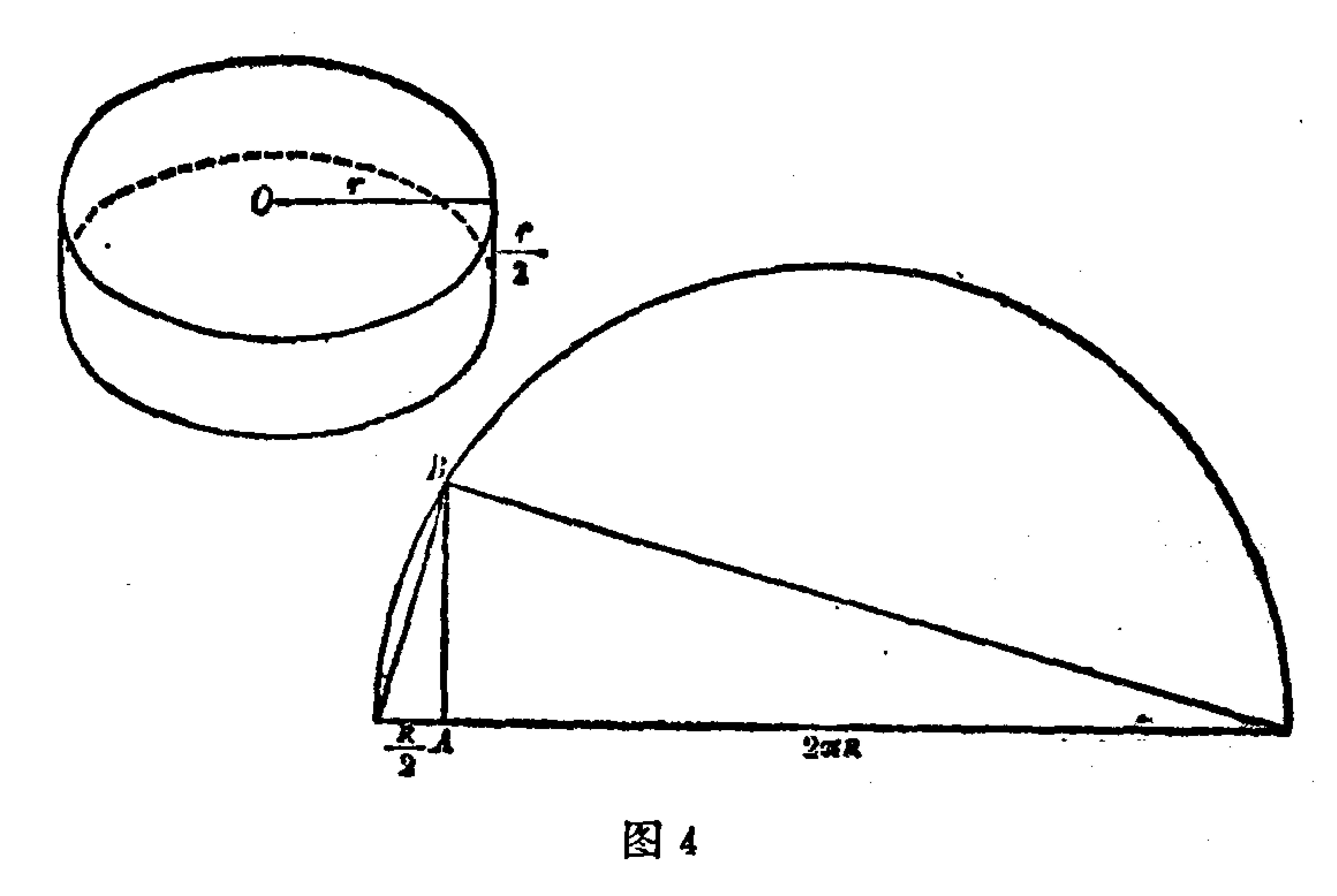


图 4

以半径为 r 的已知圆为底作一圆柱，其高为 $r/2$.将这个圆柱在平面上滚动一周，产生一个矩形，其边长为 $r/2$ 和 $2\pi r$.以 $2\pi r+r/2$ 为直径作一半圆。在分点 A 处作一垂线交半圆于

B 点，则

$$|AB|^2=\frac{r}{2}\cdot 2\pi r=\pi r^2。$$

因此，以 $|AB|$ 为边长的正方形的面积就是已知圆的面积。但是这种方法也不符合圆规直尺作图的规定。如果设已知圆的半径为 1，则面积为 π。于是要作的正方形的边长 $x=\sqrt{\pi}$。直到 1882 年，林德曼（F · Lindemann）证明了 π 是超越数以后，才知道限用圆规直尺实现化圆为方也是不可能的。

（四）**作正 n 边形**。这等价于把整个圆周 n 等分。早在古希腊的欧几里得时期，人们就知道边数为

$$3,5,15,2^n,2^n\cdot 3,2^n\cdot 5,2^n\cdot 15,$$

（n 是任意自然数）的正多边形是可作的。但在以后的二千多年的时间内却毫无进展，甚至数学家们一致声称不存在其它可作的正多边形了！在这个问题上，第一个作出卓越贡献的当推十八世纪末的德国天才数学家高斯。1796 年，这位年仅 19 岁的大学生限用圆规直尺作出了正十七边形。当时，高斯兴致冲冲地去告诉他的导师，然而得到的竟是冷嘲热讽。因为这个发现太出乎意料了，使人难以相信。由于这位教授也曾炫耀过他的诗集，于是高斯回敬他是“数学家中最好的诗人和诗人中最好的数学家”。为了永远纪念高斯在青年时代的这个重要发现，1855 年他逝世后，在他的母校哥廷根大学建立了以正十七边形棱柱为台座的高斯象。此外，高斯还进一步断言：一个正 n 边形可作当且仅当 $n=2^e p_1 p_2\cdots p_s$，这里 e 是任意自然数或 0，$p_1,\cdots,p_s$ 是 s 个两两不同的形如 $2^{2^s}+1$ 的素数。当时，高斯仅证明了这一断言的充分性，其必要性是由旺采尔（P · L · Wantzel，1814-1848）于 1837 年证明的。我们

也将用伽罗瓦理论证明高斯的这一结论。

解决这些乍看起来似乎并不困难的问题，怎么会经历如此漫长而又艰难的岁月呢？二千多年来，曾有无数人将自己的聪明才智倾注在这些难题上，但未得到丝毫结果，其原因就是缺乏一些新的工具。拉格朗日使用的工具——预解式，在 $n=5$ 时失效了。直到伽罗瓦等人找到了真正有效的工具——抽象代数学中的群、环和扩域理论，这些长期折磨着人们的难题才一一迎刃而解。这就是我们在下两章中要讲的内容。由于这些内容涉及到许多抽象代数的重要概念，这些概念不但对解决上述古典难题必不可少，而且也是抽象代数这门学科的基础，因此我们打算由浅入深地将它们向读者作些简要的介绍。

第二章　群的基本知识

§1　集合与映射

抽象代数学有两块重要的基石。一块叫集合。另一块叫映射。

集合这个概念大家是很熟悉的。例如，某些数可组成一个数的集合，某些平面向量或空间向量可组成向量集合。另外，还有矩阵集合，多项式集合，函数集合，点集合，线集合，面集合等等。在本书中除了要用到这些常见的集合以外，主要是讨论由某些变换组成的集合。关于变换的定义将在本节末引进。通俗地说，把某些(数量上可为有限或无限)研究对象放在一起，就组成了一个集合 S，而且我们总可判定任一对象是否属于某个给定的集合 S。例如，令 Z 是由全体整数组成的集合。任给一数，如果它是整数，则属于 Z，否则就不属于 Z。属于集合 S 的对象称为 S 中的*元素*。在对集合作一般性讨论时，我们不再关心那些元素究竟代表着什么东西。因此，元素是个抽象概念，它可以是任意需要研究的对象。特别需要指出的是：集合中的元素本身也可以是集合。例如，一所学校的所有班级组成一个集合，而每个班级又是由该班全体学生所组成的集合。

现在，我们把集合论中常用记号先向读者介绍一下。如

果 a 是集合 S 中的一个元素，则记为 $a\in S$；否则，记为 $a\notin S$。设 A 和 B 是两个集合。如果 A 中任一元素都在 B 中，则记为 $A\subseteq B$ 或 $B\supseteq A$，此时，称 A 是 B 的子集，B 是 A 的扩集。如果 A 中元素都在 B 中，且至少存在一个元素 $b\in B$ 而 $b\notin A$，则称 A 是 B 的真子集，B 是 A 的真扩集，记为 $A\subset B$ 或 $B\supset A$。如果 $A\subseteq B$ 且 $B\subseteq A$，则称这两个集合相等，记为 $A=B$。今后，我们将经常采用证明 $A\subseteq B$ 和 $B\subseteq A$ 的途径得出 $A=B$ 的结论。既属于 A 又属于 B 的元素集合称为 A 与 B 的交集，记为 $A\cap B$。由 A 和 B 的所有元素组成的集合称为 A 与 B 的并集，记为 $A\cup B$。常用的集合表示法有以下两种。如果 S 中仅包含很少几个元素，则常采用枚举法。例如，从 0 到 5 的所有整数组成的集合可记为 $S=\{0, 1, 2, 3, 4, 5\}$。不过，在不会引起误会的前提下，也可用 $S=\{1, 2, \cdots, n\}$ 表示 1 到 n 的所有自然数，尽管 n 可以是很大很大的自然数。对于一般集合(有限集或无限集)，常采用特性表示法。例如，从 0 到 100 的所有偶数组成的集合可记为

$$S=\{x \mid x\text{ 是偶数，满足 } 0\leqq x\leqq 100\}。$$

又如行列式为 1 的 n 阶实矩阵全体组成的集合可记为

$$S=\{A \mid A\text{ 为 } n\text{ 阶实矩阵，}\det A=1\}。$$

这里，x 和 A 都是属于这个集合的元素名称或记号，写在竖号的左边。在竖号右边的是一张表示该特性的“说明书”，根据这张说明书可确定某个数 x 或矩阵 A 是否属于所讨论的集合 S。当然，为了保证集合中元素的确定性，不允许出现那种含糊不清的说明书。在特性表示法中，也可不写出元素的名称。例如，

$$S=\{\text{实系数一元多项式}\}$$

就是表示由所有的系数为实数的一个变元的多项式组成的集

合。在本书中，我们约定采用以下记号代表有关集合，使用时就不一一说明了：

$Z=\{$整数$\}$，　$Q=\{$有理数$\}$，

$R=\{$实数$\}$，　$C=\{$复数$\}$，

$F[X]=\{$数域 F 上一元多项式$\}$ ①，

$M_n(R)=\{$实系数 n 阶方阵$\}$，

$GL_n(R)=\{$实系数 n 阶可逆阵$\}$，

$SL_n(R)=\{$行列式为 1 的实系数 n 阶阵$\}$，

这里的花括号都有"全体"的意思。若 S 是某一包含数 0 的数集，去掉 0 后剩下的集合记为 S^*。例如，Q^*表示非零有理数全体，R^*表示非零实数全体，等等。如果 S 是有限集，则用$|S|$表示 S 中所含元素的个数。

在引进映射的概念之前，让我们先回忆一下单值函数的概念。例如，　$y=4x^3+5x^2-6x+3$，　$y=\sqrt{x}$，　$y=e^x$，$y=\sin x$，还有符号函数 $y=\mathrm{sgn}(x)$，它对正实数 x 取值 1；对 $x=0$ 取值 0；对负实数 x 取值-1。这些五花八门的函数有一个共同之处：对于定义域中任意一个 x 值，都可根据函数表达式求出唯一的 y 值与之对应。我们称它们为单值函数。易见，$y=\pm\sqrt{x}$，$y=\mathrm{arctg}\,x$ 都不是单值函数。$y=\ln x$ 是单值函数，但是负数无对数。一般地，用 $y=f(x)$ 表示 y 是 x 的(单值)函数。其实，就其本质来说，函数关系不必写得如此烦琐，仅写 $f(x)$ 即可；给定一个 x 值，就可唯一确定函数值 $f(x)$。这件事也可表示成

$$f: x\to f(x) \quad \text{或} \quad x \xrightarrow{f} f(x) \tag{1}$$

① 详见第三章§1。

读作函数关系 f 把 x 变为 $f(x)$。这样就把 f 和 x 拆开了，f 仅是一个函数记号。它的意思是，根据函数关系 f，对于任一 x 值都可唯一确定函数值 $f(x)$。所以这个 f 实际上是一个对应的法则。上述表示法(1)仅说出了元素之间的关系，有时还需要说明两个集合之间的关系。例如，给定某个函数关系 f，如果对任一实数 x，得出的 $f(x)$ 仍是实数，就说 f 确定了实数集 R 到 R 的一个映射，记为

$$f: R \longrightarrow R \quad 或 \quad R \xrightarrow{f} R。$$

在上述各例中，$\sqrt{x}$ 是非负实数集 R^+ 到 R^+ 的映射（当然也是复数集 C 到 C 的映射），符号函数 $\mathrm{sgn}(x)$ 是 R 到三元集 $\{-1, 0, 1\}$ 的映射，$\sin x$ 是 R 到实闭区间 $[-1, 1]$ 的映射。读者试对 e^x 和 $\ln x$ 作出相应的叙述。

映射离不开集合，关于两个集合之间的映射的定义是

定义 1·1　设 A 和 D 是两个集合。如果存在某个对应法则 f，使对任一 $a \in A$，都能唯一确定 D 中一个元素 d 与之对应，则称 f 是 A 到 D 的一个**单值映射**，记为

$$f: a \longrightarrow d \quad 或 \quad a \xrightarrow{f} d \quad 或 \quad d = a^f。$$

称 d 是 a 在 f 之下的**象**，称 a 是 d 在 f 之下的某个**原象**。

注意，A 中不同的元素在 D 中可以有同一个象。例如，$x \to \sin x$ 是 R 到 $[-1, 1]$ 的单值映射，不同的 x 可以有相同的正弦值。又如 $A \to \det A$ 是 $M_n(R)$ 到 R 的映射，但不同的矩阵可以有相同的行列式。因为我们只讨论单值映射，以后就省略“单值”两字了。一个 A 到 D 的对应法则称得上是一个映射，它必须满足三个条件：A 中任一元素都有象，象必在 D 中，且象是唯一的。此三要素缺一不可！映射的第三

种表示法$d=a^f$是本书中采用的主要记号。把映射 f 写在 a 的右肩上表示 a 在 f 之下的象。于是函数 $f(x)$ 作为一种特殊的映射，函数值 $f(x)$ 就是 x^f。这种写法初看起来很别扭，但读者将会发现，在很多场合下，它既是方便的，又是合理的，所以必须习惯于这种记号。

设 f 是 A 到 D 的映射。如果对任一 $d\in D$，必存在 $a\in A$ 使 $d=a^f$，则称 f 是 A 到 D 的满射，或说 f 是 A 到 D 上的映射。如果对 A 中不同的元素，在 f 之下有不同的象，即 $a^f=b^f$ 当且仅当 $a=b$，则称 f 是 A 到 D 的单射。如果 f 既是满射，又是单射，就称为双射或一一对应，此时，D 中任一元素 d 必是 A 中某一元素 a 的象，且 a 是 d 的唯一的原象。特别地，当 A 和 D 都是有限集合时，所含元素的个数必相等。学到这里，读者应能造出一些映射，并判定哪些是单射、满射或双射。映射概念是函数概念的推广，这是一个很重要的"抽象"。

在定义 1.1 中，A 和 D 可以是两个任意的集合。特别地，如果 $D=A$，即 f 是 A 到 A 自身的映射，则称 f 是 A 中的变换。A 到 A 的满射称为满变换，单射称为单变换，一一映射称为一一变换。有一种特殊的变换称为恒等变换，它保持 A 中任一元素不变：$a\to a$，$\forall a\in A$。这里的记号"$\forall$"具有"所有"、"对一切"的意思。常用 1_A 表示 A 中的恒等变换。在不会引起混淆时，就用 1 表示恒等变换。当然，它并不是数字 1。易见，恒等变换必是一一变换。

设 A 是某个取定的集合。考虑由 A 中变换全体所成的集合 T。对于 σ，$\tau\in T$，可定义 σ 与 τ 的乘积 $\sigma\tau$ 是

$$a^{\sigma\tau}=(a^\sigma)^\tau,\qquad \forall a\in A。$$

这就是说，对于 A 中任一元素 a，规定 a 在 $\sigma\tau$ 之下的象是 $(a^{\sigma})^{\tau}$，即先求出 a 在 σ 之下的象 a^{σ}，再求出 a^{σ}在 τ 之下的象 $(a^{\sigma})^{\tau}$。易见，$\sigma\tau$ 也是 A 中变换。变换的乘积是复合函数概念的推广和抽象。两个函数 f 和 g 的复合函数 fg 是新函数

$$(fg)(x)=f[g(x)],$$

这里，在 fg 中，g 后写但先求值 $g(x)$，f 先写，但后求值 $f[g(x)]$，这就给了人们一种颠倒的感觉。如果采用我们的记号，则 f 和 g 的复合函数应是

$$x^{gf}=(x^{g})^{f},$$

这样，求值次序与书写次序就一致了！众所周知，$(fg)(x)$与 $(gf)(x)$ 未必是同一个函数，而函数是映射的特例，所以两个映射 σ 和 τ 的乘积 $\sigma\tau$ 与 $\tau\sigma$ 也未必相等。因此，在作变换的乘积时，必须讲清楚是 σ 与 τ 相乘还是 τ 与 σ 相乘。这与数的乘法有本质性不同。若 σ 是 A 中任一变换，1 是 A 中恒等变换，则由乘积的定义立刻得到

$$\sigma\cdot 1=1\cdot\sigma=\sigma,$$

所以恒等变换又称为单位变换。

设 φ, σ 和 τ 是集合 A 中的三个变换，则从下图可直观地看出变换的乘法满足结合律：$(\varphi\sigma)\tau=\varphi(\sigma\tau)$

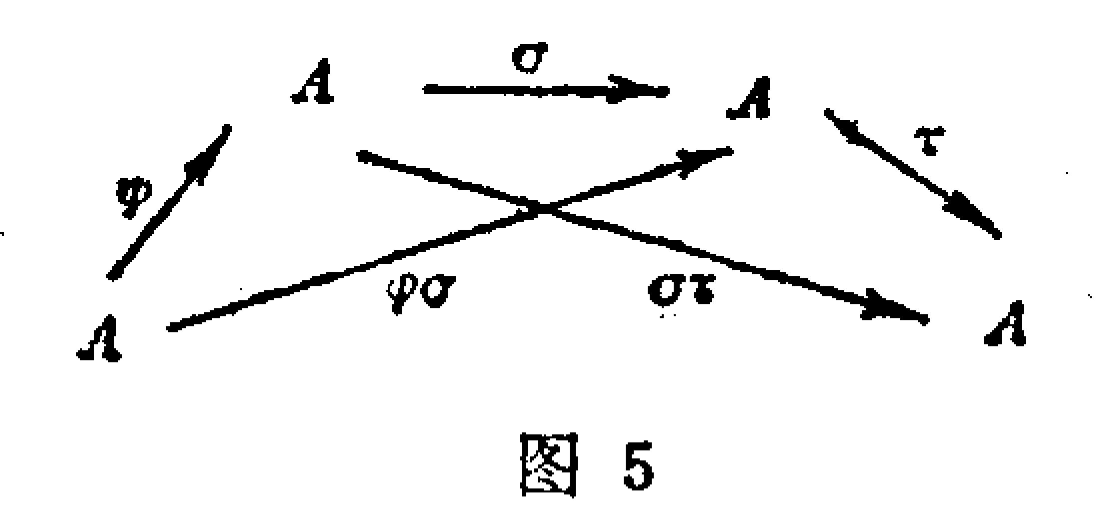


图 5

即先求出 φ 与 σ 之积 $\varphi\sigma$，再求与 τ 之积，或者，先求出 σ

与τ之积$\sigma\tau$，再求φ与$\sigma\tau$之积，所得的结果是一样的．读者应该记住这件事情，以后用到时就不再说明了．

§2 群的定义

群的概念属于代数学的范畴，它是伽罗瓦在十九世纪三十年代提出的，但是，迟至下半世纪才真正被人们所理解和接受。至今一百多年来，它在数学的各个分支和物理学、力学、化学、生物学、计算机科学等方面都有越来越广泛的应用。同时，实际应用的需要又促使群论本身不断得到丰富、深刻和提高。可以预见，以群论为基础的抽象代数学必将与拓扑学一起成为各个数学学科的基础知识和基本工具。这无非有两个方面的原因。其一，群论作为一种工具，能在较高的观点上，把一些形式上很不相同的代数系统，撇开其个性，抽出其共性，用统一的方法描述、研究和推理，从而得到一些反映事物本质的结论，再把它们应用到那些代数系统中去．高度的抽象产生了广泛的应用。其二，可以根据需要构造出一种新的群，再利用群的性质，使一些疑难问题迎刃而解．因为群的结构往往体现着事物的本质．伽罗瓦就是运用置换群理论解决了高次代数方程根号求解等疑难问题的。

群虽然是一个抽象概念，但却有着无数的实际背景。不知你是否意识到，在数学中，在其它学科中，甚至在日常生活中，到处都有群。例如，任意两个整数相加仍是整数，整数的相反数仍是整数，0是整数，我们就说，整数全体Z是一个加法群。再考虑非零有理数全体Q^*。两个非零有理数相乘是非零有理数，任意一个非零有理数的倒数必是非零有理数，1是

非零有理数，我们说Q^*是一个乘法群。以后我们将要说明，钟面上的12个钟点数，每年中的12个月，每星期中的7天，每小时的60分钟等等都是加法群。另外，空间中的刚体运动，晶体的结构，化学分子的结构，生物的形态等等也都可用群论方法来研究。总之，群是某个集合，其中定义了某个运算，另外还满足某些条件。群的确切定义是

定义 2·1　设G是某个非空集合。在G中定义着某个运算“·”。如果满足以下条件

(1)封闭性：对任意$a,b\in G$，有唯一的运算结果$a\cdot b\in G$；

(2)结合律：对任意a，b，$c\in G$，有$(a\cdot b)\cdot c=a\cdot(b\cdot c)$；

(3)单位元：存在某个元素$e\in G$，使得对任何$a\in G$，都有$e\cdot a=a\cdot e=a$；

(4)逆元：对任一$a\in G$，必存在某个元素$b\in G$，使$a\cdot b=b\cdot a=e$，

则称G关于这个运算“·”构成群，记为$(G,\ \cdot)$。

满足第(3)个条件的那个元素e称为单位元，每个群只有一个单位元。一个元素是不是单位元，当然与具体的运算有关。如果运算是数的加法，则单位元是数0，$0+a=a+0=a$。如果运算是数的乘法，则单位元是数1，$1\cdot a=a\cdot 1=a$。满足第(4)个条件的元素b称为a的逆元，它由a唯一确定，通常记为a^{-1}，有$a\cdot a^{-1}=a^{-1}\cdot a=e$。对于数的加法来说，$a$的逆元是$a$的相反数$-a$，$a+(-a)=(-a)+a=0$。对于数的乘法来说，$a$的逆元是$a$的倒数$1/a$，$a(1/a)=(1/a)a=1$。易见，只有非零数才有逆元。在这里需要强调指出，在群的定义中，运算“·”是一个抽象的记号，它可以代表加法，可以代表乘法，也可以代表任何其它运算，具体的群需要有具体的规定。为了便于作统一的讨论，我们就把它称为“乘法”，而且经常

省略这个乘号，干脆把 $a\cdot b$ 缩写为 ab。但必须注意，若是加法，则它表示 $a+b$。严格说来，讲到群必须讲明是哪个集合和哪个运算。例如，整数集 Z 关于加法成群，需写成 $(Z, +)$。由于不等于 ±1 的整数的倒数一定不是整数，所以 Z 关于乘法不成群。但是，群的这种带有圆括号的写法毕竟是个累赘，因此，在不会引起误会的前提下，或者所讨论的命题是否正确并不依赖于运算的具体规定时，我们径直用 G 表示群 $(G, \cdot)$，它的含义就是 G 关于某个运算成群。例如，可把群 $(Z, +)$ 简写成群 Z。如果群 G 中仅含 n 个元素，则称 G 是 n 阶群，并记为 $|G|=n$。我们称这种群为**有限群**。不是有限群的群称为**无限群**。

对照这个定义可以验证，偶数全体是无限加法群，但不是乘法群。奇数全体、自然数全体既不是加法群，又不是乘法群。Q^* 是无限乘法群，但 Q 不是乘法群。如果把钟面上的 12 点规定念作零点，则 12 个钟点数 $\{0,1,2,\cdots\cdots,11\}$ 就是一个 12 阶加法群，0 是单位元。由 $3+9=12=0$ 知，3 的逆元是 9，9 的逆元是 3。同理，若把星期日念作星期零，则一周中的 7 天就是 7 阶加法群。

以上考虑的集合 G 都是数集，而且运算是数的加法或乘法。但是，还存在大量的群 $(G, \cdot)$，其中 G 不再是数集了。例如，实系数多项式全体 $R[x]$ 关于多项式加法成群，但关于多项式乘法不成群①。$M_n(R)$ 关于矩阵加法成群，关于矩阵乘法不成群。$GL_n(R)$ 和 $SL_n(R)$ 关于矩阵乘法都成群，但关于矩阵加法却不成群。

设 G 是群。G 中任一元素 a 必有逆元 a^{-1}：$aa^{-1}=a^{-1}a=$

① 关于多项式的运算见第三章 §1。

e. 根据这一事实可以证明在群中消去律成立，即若有 $ab=ac$，两边左乘a^{-1}，得 $eb=ec$，$b=c$。同理，可由 $ba=ca$ 推得 $b=c$. 由于对 $a, b\in G$ 未必有$ab=ba$，所以当$ab=ca$时未必有 $b=c$。同理，也不能由 $abc=dbf$ 推出 $ac=df$。因此，在群中只有位于等式两边同侧端点的相同元素才能被消去。运用群中消去律可得出有限群的一个重要性质。设 $G=\{a_1, a_2, \cdots\cdots, a_n\}$ 是 n 阶群。任意取定某个 $a_i\in G$，把它左乘 G 中所有的元素，得到集合

$$G_l=\{a_i a_1, a_i a_2, \cdots\cdots, a_i a_n\},$$

根据群中乘法封闭性知，$G_l\subseteq G$。如果在 G_l 中某两个元素相同：$a_i a_j=a_i a_k$，则由消去律得 $a_j=a_k$，所以 G_l 中 n 个元素两两不同，于是必有 $G_l=G$。同理可证

$$G_r=\{a_1 a_i, a_2 a_i, \cdots\cdots, a_n a_i\}=G.$$

§3 变换群与置换群

在伽罗瓦理论中主要考虑变换群，其研究对象是某些变换，而变换就是某个集合中的映射。设 S 是某个取定的集合。把 S 中全体变换所成的集合记为 T。在 T 中已定义了变换的乘法：对 $\sigma, \tau\in T$，规定

$$a^{\sigma\tau}=(a^{\sigma})^{\tau}, \quad \forall a\in S,$$

那末要问 $(T, \cdot)$ 是否成群呢？这里运算“·”取为变换的乘法。显然，S 中的变换的乘积仍是 S 中的变换，变换的乘法满足结合律，恒等变换 1 是 T 中单位元。可惜第(4)个条件未

必满足，即对 $\sigma\in T$，未必存在逆变换 $\tau\in T$ 使 $\sigma\tau=\tau\sigma=1$。对此，我们只要举出一个反例就够了。例如，取 σ 是这样一个变换，它把一切 $x\in S$ 都变为 S 中某个确定的元素 a，即 $x^{\sigma}=a$，$\forall x\in S$。如果存在 $\tau\in T$ 使 $\sigma\tau=1$，则应有 $x=x^{\sigma\tau}=a^{\tau}$，$\forall x\in S$。这说明任一 $x\in S$ 都是这个 a 在 τ 之下的象。因此，当 $|S|\geqslant 2$时，就与象的唯一性要求相抵触，这个 τ 不是单值变换。由此可见，这个 σ 不存在逆变换。

那末，哪些变换一定存在逆变换呢？我们证明：某个变换存在逆变换，当且仅当它是一一变换。这种存在逆变换的变换称为**可逆变换**。设 σ 是可逆变换，则存在 $\tau\in T$ 使 $\sigma\tau=\tau\sigma=1$。任取 $a'\in S$，记 $(a')^{\tau}=a$，则 $a\in S$，且 $a^{\sigma}=(a')^{\tau\sigma}=a'$，这说明 σ 是满射。又若对 a，$b\in S$ 有 $a^{\sigma}=b^{\sigma}$，则 $a^{\sigma\tau}=b^{\sigma\tau}$，即 $a=b$，这又说明 σ 是单射。于是，σ 是一一变换。反之，设 σ 是一一变换，即是 S 到 S 的双射，则对任一 $a'\in S$，必存在唯一的 $a\in S$ 使 $a^{\sigma}=a'$。如令：$\tau:a'\to a$，这里 $a^{\sigma}=a'$，则 τ 也是 S 中的一个变换。由 $a^{\sigma\tau}=(a')^{\tau}=a$，$\forall a\in S$知，$\sigma\tau=1$。又由 $(a')^{\tau\sigma}=a^{\sigma}=a'$，$\forall a'\in s$知，$\tau\sigma=1$。所以 σ 是可逆变换。这样，可逆变换与一一变换就是一回事了！集合 S 上的可逆变换全体关于变换乘法成群，称为集合 S 上的**变换群**①。

在伽罗瓦理论中起关键作用的是一种特殊的变换群——置换群，它就是仅含 n 个文字（或序号）的有限集合 $S=\{1, 2, \cdots\cdots, n\}$ 上的变换群。现在，我们来详细地说明它的构造。

若 $n=1$，则 $S=\{1\}$ 上的变换仅有一个，即恒等变换。逐个检验群的四个条件可知，$S_1=\left\{\begin{pmatrix}1\\1\end{pmatrix}\right\}$也构成群，这是只含

① 一般书上是把它的子群称为变换群。

一个文字的集合 S 上的变换群，这里 $\begin{pmatrix}1\\1\end{pmatrix}$ 表示把 1 变为 1 的恒等变换。

若 $n=2$，则 $S=\{1,2\}$ 上的变换仅有以下两个：一个是恒等变换，它保持 1 和 2 不变；另一个是把 1 变为 2，2 变为 1。这两个都是一一变换，依次记为 $\begin{pmatrix}1&2\\1&2\end{pmatrix}$ 和 $\begin{pmatrix}1&2\\2&1\end{pmatrix}$。在这种记号中，第一行就是 S 的元素，且按自然顺序排列。位于这行中每个文字下面的对应文字就是它在此变换之下的象。例如，$\begin{pmatrix}1&2\\2&1\end{pmatrix}$ 表示这个变换把 $1\to2$，$2\to1$。当然，就确定某个一一对应关系来说，$\begin{pmatrix}1&2\\1&2\end{pmatrix}$ 与 $\begin{pmatrix}2&1\\2&1\end{pmatrix}$ 没有丝毫区别，都表示恒等变换。同理，$\begin{pmatrix}1&2\\2&1\end{pmatrix}$ 与 $\begin{pmatrix}2&1\\1&2\end{pmatrix}$ 都表示互换 1 与 2 的变换，所以 $S=\{1,2\}$ 上的变换群可记为

$$S_2=\left\{\begin{pmatrix}1&2\\1&2\end{pmatrix},\ \begin{pmatrix}1&2\\2&1\end{pmatrix}\right\},$$

它是 2 阶群。这个群的几何背景如下：在平面上任取一个线段，其端点分别标为 1 与 2。变动它的状态，使其所占平面位置不变，至多改变其端点的序号。易见，这种变换仅有 S_2 中的两个：保持 $\overset{1}{\cdot}$———$\overset{2}{\cdot}$ 不变，或把 $\overset{1}{\cdot}$———$\overset{2}{\cdot}$ 变为 $\overset{2}{\cdot}$———$\overset{1}{\cdot}$。

若 $n=3$，可证 $S=\{1,2,3\}$ 上的一一变换共有以下六个：

$$S_3=\left\{\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix},\ \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix},\ \begin{pmatrix}1&2&3\\3&1&2\end{pmatrix},\right.$$

$$\left.\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix},\ \begin{pmatrix}1&2&3\\3&2&1\end{pmatrix},\ \begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}\right\}.$$

它们相当于把顶点编号为 1，2，3 的平面正三角形作如下变

换，不变其平面位置，至多使顶点编号有所变动：

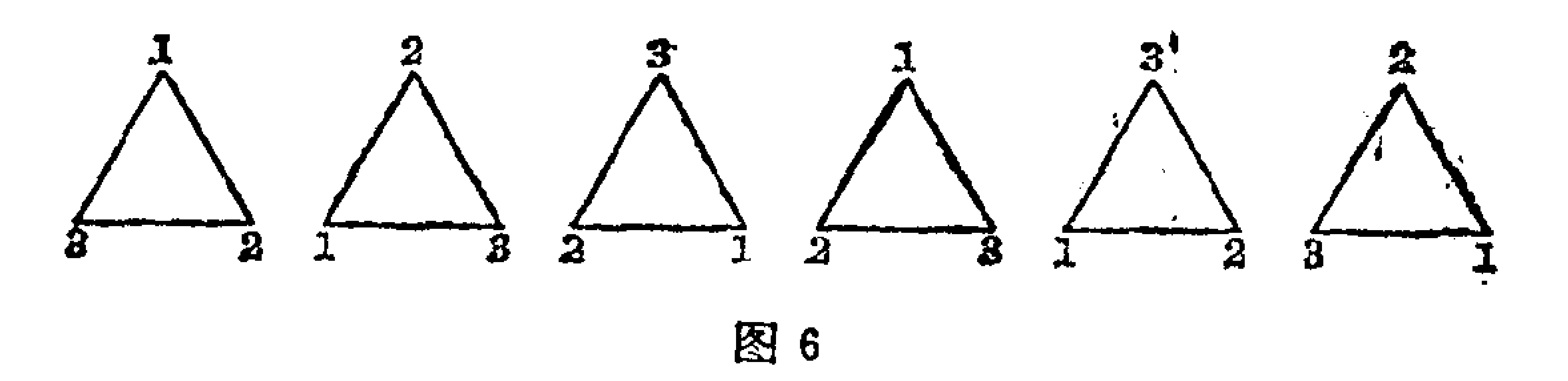


图 6

这里仍然认为

$$\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix},\begin{pmatrix}2&3&1\\3&1&2\end{pmatrix},\begin{pmatrix}3&1&2\\1&2&3\end{pmatrix},\begin{pmatrix}1&3&2\\2&1&3\end{pmatrix}$$

$$\begin{pmatrix}2&1&3\\3&2&1\end{pmatrix},\begin{pmatrix}3&2&1\\1&3&2\end{pmatrix}$$

都代表同一变换：$1\to2$，$2\to3$，$3\to1$。因为上述 S_3 中的六个变换是 $S=\{1,\ 2,\ 3\}$ 上仅有的一一变换，所以它们关于变换乘法必定成群。对于变换的这种新记号，我们应该具体地熟悉一下两个变换的乘法是如何计算的。例如

$$\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}=\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}。$$

计算过程是这样的：第一个变换把 1 变成 3，接着第二个变换又把这个 3 变为 3，所以它们的乘积把 1 变为 3。同理，它们的乘积把 2 变为 2，3 变为 1，因此，相乘结果必是 $\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}$。类似地，

$$\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}=\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix},$$

由此也可看出，变换的乘积与它们相乘的次序有关，而且求变换的次序与书写次序一致。

够了！我们不再对 $n=4,\ 5,\ \cdots\cdots$ 等情况一一细说了。从具体到抽象，从特殊到一般，让我们一跃而考虑任意自然数

n 的情形．把 $S=\{1, 2, \cdots, n\}$ 上的一一变换全体记为 S_n，它关于变换乘法成群．S_n 中元素的一般形状是

$$\begin{pmatrix} 1 & 2 & \cdots\cdots & i & \cdots\cdots & n \\ j_1 & j_2 & \cdots\cdots & j_i & \cdots\cdots & j_n \end{pmatrix}.$$

它表示把 $1\to j_1$，$2\to j_2$，……，$i\to j_i$，……，$n\to j_n$，而 $j_1 j_2\cdots j_n$ 是 $1, 2, \cdots, n$ 的任一排列，即 $j_1, j_2, \cdots, j_n$ 都是 1 到 n 之间的某个自然数，而且所取的数没有两个是重复的。这好比把点号是 1 到 n 的 n 张牌任意洗乱后撒开来排成一行一样。通常把 n 元有限集合上的一一变换称为 n 元**置换**。由于它的几何背景是把平面正 n 边形的 n 个顶点作一些置换，保持其平面位置不变，也就是说，它是一种几何对称变换，所以置换又称为**对称**，S_n 就称为 n **次对称群**。因为 n 个文字的各种排列共有 $n!=1\cdot2\cdot3\cdot\cdots\cdot n$ 种，所以 S_n 是 $n!$ 阶群。伽罗瓦依凭着这个群解决了代数方程根号求解的问题，因此，我们要用较大的篇幅研究它。

我们采用的记号，不但含义应该确切，没有两义性，而且应力求书写简洁，使用方便。置换的上述写法，则令人很不满意。一则，每个置换都要写出上下两行，这太占篇幅．再则，第一行千篇一律都是从 1 排到 n，文字与位置的编号一致，这本身就暗示着记号可以简化。例如，在 S_3 中，置换 $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$ 仅把 1 与 2 互换一下而保持 3 不变，所以就可把它简写为 $(1\ 2)$，它的含义是把前一个文字 1 变为后一个文字 2，再把尾巴上的文字 2 变为头部的文字 1，不把 3 写出就表示 3 保持不变。又如，在 S_4 中，$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix}$ 可简记为 $(1\ 2\ 4)$，它表示把 $1\to2$，$2\to4$，$4\to1$，而保持 3 不变。

另外，恒等变换不变任何文字，但总不能一个文字都不写出，于是干脆把它记作(1)，它表示不变任何文字。于是3次对称群可记为：

$$S_3=\{(1),(1\ 2\ 3),(1\ 3\ 2),(2\ 3),(1\ 3),(1\ 2)\}。$$

引进这些新记号后，置换的乘法也简化了。例如，

$$(1\ 3\ 2)(1\ 2)=(1\ 3),\quad (1\ 2)(1\ 3\ 2)=(2\ 3)。$$

再如在 S_6 中，

$$(1\ 4\ 5\ 6\ 2\ 3)(3\ 5\ 4\ 2)=(1\ 2\ 5\ 6\ 3)。$$

它是这样算出来的：经过先左后右两个置换把 $1\to4\to2$，$2\to3\to5$，$5\to6\to6$，$6\to2\to3$，$3\to1\to1$，所以相乘结果是 $(1\ 2\ 5\ 6\ 3)$，不变4。上述这种圆括号表示的置换称为轮换，这是由于它的变换方式是把前一个变为后一个，且头尾相连，好象时针在钟面上轮回转圈一般。因此，

$$(1\ 2\ 5\ 6\ 3)=(2\ 5\ 6\ 3\ 1)=(5\ 6\ 3\ 1\ 2)=(6\ 3\ 1\ 2\ 5)=(3\ 1\ 2\ 5\ 6),$$

它们都代表同一个轮换。再考虑 S_4 中的如下置换 $\begin{pmatrix}1&2&3&4\\3&4&1&2\end{pmatrix}$，它是互换1与3和互换2与4的结果。这说明我们可把这四个文字分成两组：{1，3}和{2，4}，它们在变换时互不相干，可分别考虑。我们把这一置换简记为(1 3)(2 4)。因为这两个轮换没有公共文字，它们相乘的次序是可以交换的，所以也可写成(2 4)(1 3)。这说明，原来的四元置换可分解成两个二元轮换的乘积。

一般地，如下特殊的 n 元置换

$$\sigma=\begin{pmatrix}\cdots\cdots i_1\cdots\cdots i_2\cdots\cdots i_{k-1}\cdots\cdots i_k\cdots\cdots\\ \cdots\cdots i_2\cdots\cdots i_3\cdots\cdots i_k\quad\cdots\cdots i_1\cdots\cdots\end{pmatrix}$$

(其中没有写出来的都是在σ之下保持不变的文字)可简写为

$$\sigma=(i_1\ i_2\ \cdots\ i_{k-1}\ i_k),$$

它表示 $i_1\to i_2$, $i_2\to i_3$, ……, $i_{k-1}\to i_k$, $i_k\to i_1$。我们把它称为 k-轮换,k 表示它的长度。例如,(1 2 3) 是 3-轮换,(1 5 2 3)是 4-轮换等等。特别,2-轮换 $(i\ j)$ 称为对换,它仅互换 i 与 j,而保持其它所有文字不变。可以断言:任一置换必可唯一地分解成若干个互不相交(即没有公共文字)的轮换之积,这些轮换因子的书写次序可以任意调动,也就是可以交换。要证明这个结论并不困难,下述例子的分解方式具有普遍性:

$$\begin{pmatrix}1&2&3&4&5&6&7&8&9\\4&7&6&5&1&2&3&9&8\end{pmatrix}=(1\ 4\ 5)(2\ 7\ 3\ 6)(8\ 9)。$$

其分解方法是从 1 出发,得 1→4→5→1,一旦有数字重复出现(例如 1)就关门,形成一个轮换因子 (1 4 5),再从不在这个轮换中出现的最小文字,例如 2 出发,得2→7→3→6→2,又形成(2 7 3 6),最后由8→9→8得(8 9)。这样,这三个轮换因子无公共文字,彼此可交换,而且在不计各轮换的书写次序时,这种分解式是唯一的。

进一步,每个轮换又都可拆写成若干个对换之积,不过,这些对换因子必有公共文字,因此,相乘次序不能调动。事实上,下列等式

$$\begin{aligned}(i_1\ i_2\cdots i_k)&=(i_1\ i_2)(i_1\ i_3)\cdots\cdots(i_1\ i_k)\\&=(1\ i_1)(1\ i_2)\cdots\cdots(1\ i_k)(1\ i_1)\end{aligned}$$

说明任一 k- 轮换必可表成 $k-1$ 或 $k+1$ 个对换之积,且轮换

的对换分解式未必唯一。进一步，由于对任意 i 和 j，必有 $(i\,j)(i\,j)=(1)$，所以这两个对换必可紧挨在一起插入对换分解式中的任意一个地方。例如，

$$(1523)=(15)(12)(13)=(24)(24)(15)(12)(13)$$
$$=(15)(24)(24)(12)(13)$$
$$=(15)(12)(24)(24)(13)=\cdots\cdots$$

尽管如此，我们仍可证明，在 k-轮换的任一对换分解式中所含对换因子的个数的奇偶性都是一致的，而且就是 $k-1$ 的奇偶性。为此，考虑 k-轮换 $(i_1 i_2 \cdots i_k)$ 在范达蒙行列式

$$V(x_{i_1}, x_{i_2}, \cdots, x_{i_k})=\begin{vmatrix} 1 & \cdots & 1 & \cdots & 1 & \cdots & 1 \\ x_{i_1} & \cdots & x_{i_j} & \cdots & x_{i_l} & \cdots & x_{i_k} \\ x_{i_1}^2 & \cdots & x_{i_j}^2 & \cdots & x_{i_l}^2 & \cdots & x_{i_k}^2 \\ \vdots & & \vdots & & \vdots & & \vdots \\ x_{i_1}^{n-1} & \cdots & x_{i_j}^{n-1} & \cdots & x_{i_l}^{n-1} & \cdots & x_{i_k}^{n-1} \end{vmatrix}$$

$$=\prod_{1\leq t<s\leq k}(x_{i_s}-x_{i_t})$$

上的作用。因为这个 k-轮换是把 $i_1\to i_2$, $i_2\to i_3$, $\cdots$, $i_{k-1}\to i_k$, $i_k\to i_1$，所以它把 $V(x_{i_1}, x_{i_2}, \cdots, x_{i_{k-1}}, x_{i_k})$ 变为 $V(x_{i_2}, x_{i_3}, \cdots, x_{i_k}, x_{i_1})$，就是把原行列式中的 x_{i_1} 换成 x_{i_2}，x_{i_2} 换成 x_{i_3}，$\cdots\cdots$，$x_{i_{k-1}}$ 换成 x_{i_k}，x_{i_k} 换成 x_{i_1}。由于范达蒙行列式必是如上式所示的 $(k-1)k/2$ 个两个变量的差因子的乘积，所以变换前后的两个行列式最多相差一个负号，而且，是否改变原行列式的正负号完全由此 k-轮换决定，与对换分

解式无关。但是，任意一个对换 $(i_j\ i_l)$ 作用在行列式上就是仅仅互换第 i_j 和 i_l 两列，行列式必定改号，所以轮换的任一对换分解式中所含对换因子个数的奇偶性必相同。既然置换 σ 可以唯一地分解成轮换之积，每个轮换又可表成对换之积，所以 σ 可分解成若干个对换之积，且所含对换因子总个数的奇偶性由 σ 唯一确定。因此，我们可把置换分成如下两大类：

定义 3·1　若置换 σ 可表成偶数个对换之积，则称 σ 是**偶置换**，否则，称为**奇置换**。

于是，长度为奇数的轮换是偶轮换，长度为偶数的轮换是奇轮换。对于给定的置换，如何确定其奇偶性呢？把置换 σ 写成互不相交的轮换之积

$$\sigma=\rho_1\rho_2\cdots\rho_s\tau_1\tau_2\cdots\tau_t,$$

其中 $\rho_1, \rho_2, \cdots, \rho_s$ 都是偶轮换，$\tau_1, \tau_2, \cdots, \tau_t$ 都是奇轮换。易见，σ 是偶置换当且仅当 t 是偶数，即长度为偶数的轮换因子有偶数个。例如，$(1\ 4\ 5)(2\ 7\ 3\ 6)(8\ 9)$是偶置换，$(1\ 4\ 5)(2\ 7\ 3\ 6)$是奇置换。

若 σ 和 τ 都是偶置换，则都可写成偶数个对换之积，所以，$\sigma\tau$ 也可写成偶数个对换之积，这说明偶置换的乘积仍是偶置换。若 σ 是偶置换，它可表成偶数个对换之积

$$\sigma=\tau_1\tau_2\cdots\cdots\tau_{2s-1}\tau_{2s}.$$

易见，任一对换 $\tau=(i\ j)$之逆 $\tau^{-1}=\tau$，且由$(\tau_1\tau_2)(\tau_2^{-1}\tau_1^{-1})=\tau_1(\tau_2\tau_2^{-1})\tau^{-1}=\tau_1\tau_1^{-1}=(1)$知$(\tau_1\tau_2)^{-1}=\tau_2^{-1}\tau_1^{-1}$，所以，

$$\sigma^{-1}=\tau_{2s}^{-1}\tau_{2s-1}^{-1}\cdots\cdots\tau_2^{-1}\tau_1^{-1}$$

仍是偶数个对换之积。这说明偶置换的逆元仍是偶置换。恒等变换$(1)=(1\ 2)(1\ 2)$当然是偶置换。所以，当 $n\geq2$ 时 S_n中

偶置换全体成群，记为 A_n，称为 n 次交错群。

§4 子群与拉格朗日定理

在上一节中已经证明了 S_n 和 A_n 关于变换的乘法都成群。但作为集合来说有包含关系 $A_n \subseteq S_n$，我们可说 A_n 是 S_n 的子群。子群的一般定义是

定义 4·1 设 $(G, \cdot)$ 是群，H 是 G 的非空子集合。如果 H 关于 G 中的运算"·"也成群，则称 H 是 G 的子群，记为 $H \leqq G$。

在集合论中，$H \subseteq G$ 表示 H 是 G 的子集合；在群论中，$H \leqq G$ 表示 H 是 G 的子群（当然，H 首先是 G 的子集合）。关于这两个记号在含义上的区别，以后我们就不再说明了。

任意一个群 G 至少有两个子群：一个是仅由单位元 e 所成的群 $\{e\}$，称为单位元群；另一个就是 G 本身，它也可看成是 G 的子群。这两个子群称为 G 的平凡子群。不是平凡子群的子群称为真子群。例如，A_n 是 S_n 的真子群，偶数加群是整数加群的真子群，等等。

设 H 是群 G 的子群。根据定义，这只不过说明 H 中有单位元 e'，且对 H 中任一元素 a，在 H 中必有逆元 a' 满足 $aa'=a'a=e'$。那末我们自然要问：这个 e' 与 G 中单位元 e 是否一致？又若 $a \in H$，a 当然也是 G 中元素，a 在 H 中的逆元 a' 是否就是 a 在 G 中的逆元 a^{-1}？可以证明，回答都是肯定的，即有

引理 设 H 是群 G 的子群，则 H 中单位元 e' 就是 G 中单位元 e。任一 $a \in H$ 在 H 中的逆元 a' 就是在 G 中的逆

元 a^{-1}。

证 因为 e 是 G 中的单位元，所以 $ee'=e'$。因为e'是 H 中单位元，又有 $e'e'=e'$，于是 $ee'=e'e'$。再右乘e' 在 G 中的逆元e'^{-1}得 $ee'e'^{-1}=e'e'e'^{-1}$，$ee=e'e$。但 e 是G中单位元，故有 $e=e'$。进一步，由逆元的定义知 $aa'=e'=e=aa^{-1}$，再左乘 a 在 G 中的逆元即得 $a'=a^{-1}$。▌

定理 4·1 设 H 是群 G 的非空子集，则 H 是 G 的子群 $\Longleftrightarrow$①(1) 对任意 $a,b\in H$，有 $ab\in H$，

(2) 对任意 $a\in H$，有 $a^{-1}\in H$。

证 必要性。设 H 是 G 的子群。由 H 是群知封闭性条件(1)满足。任取 $a\in H$。据引理知，a 在 G 中的逆元a^{-1}就是 a 在 H 中的逆元，既然 H 是群，当然，$a^{-1}\in H$，条件(2)满足。

充分性。设 H 满足条件(1)和(2)，要证 H 是群。条件(1)就是封闭性。因为$H\subseteq G$，G 中元素满足结合律，H 中元素当然也满足结合律。设 e 是 G 中单位元。任取 $a\in H$。由条件(2)知：a 在 G 中的逆元 $a^{-1}\in H$，再由条件(1)知，$aa^{-1}=e\in H$，所以这个 e 也是 H 的单位元。最后，由条件(2)知，任一 $a\in H$ 必有逆元 $a^{-1}\in H$。于是 H 成群，因而就是 G 的子群。▌

这是一个很实用的判别准则。要证明某群 G 的子集 H 是子群，只要验证这两个条件满足，而不必一一验证群的定义中的四个条件。

关于群与子群之间的关系有一个非常重要的定理——拉格朗日定理。尽管拉格朗日逝世时，作为群论创始人的伽罗

① 记号"$\Longleftrightarrow$"表示充分必要条件，也就是"当且仅当"的意思。

瓦才两岁，但拉格朗日早就有把集合划分的思想，所以后人把这个定理用他的名字来命名。

与子群密切相关的概念是陪集，我们先要把它讲清楚。设 H 是 G 的子群．任取 $a\in G$，记

$$aH=\{ah|h\in H\},$$

它是由 a 左乘 H 中每一个元素所得的集合，这个集合称为 H 在 G 中的一个**左陪集**。据 $e\in H$ 知，$a=ae\in aH$，所以由 a 确定的左陪集 aH 必包含 a。同理，对任一 $a\in G$，可定义 H 在 G 中的一个**右陪集**为

$$Ha=\{ha|h\in H\},$$

也有 $a=ea\in Ha$。这两个陪集都由一个元素 a 确定。当然，不同的元素可以确定同一个左(右)陪集．进一步可证，对 a，$b\in G$ 有

$$aH=bH\Longleftrightarrow b^{-1}a\in H,$$

$$Ha=Hb\Longleftrightarrow ba^{-1}\in H。$$

事实上，若 $aH=bH$，则对任一 $h\in H$，必存在 $h'\in H$ 使 $ah=bh'$，(注意，未必有 $h=h'$！)，两边同时左乘 b^{-1} 和右乘 h^{-1}，得 $b^{-1}a=h'h^{-1}\in H$ (因为 H 是群)。反之，设 $b^{-1}a=h\in H$，则 $a=bh$，$aH=bhH=bH$，(因为 $h\in H$ 而 H 是群，所以 $hH=H$)，于是(1)式成立。同理，可证(2)式成立。

设 H 为 G 的一个子群，那么 H 在 G 中有多少个不同的陪集呢？

定理 4·2 (拉格朗日)。设 G 是 n 阶群，H 是 G 的 m 阶子群，则 m 必整除 n。所得商数 n/m 称为 H 在 G 中的**指数**，记为 $[G:H]=n/m$。

证 设 $H=\{a_1, a_2, \cdots, a_m\}$。任取 $a\in G$。考虑左陪集 $aH=\{aa_1, aa_2, \cdots, aa_m\}$。因为在群 G 中消去律成立，所以在 aH 中的各个 aa_i 也互不相同，故对任何 $a\in G$ 都有

$$|aH|=|H|=m。$$

进一步，如果存在某个 $x\in aH\cap bH$，则存在 $h_1,h_2\in H$ 使 $x=ah_1=bh_2$，$b^{-1}a=h_2h_1^{-1}\in H$，由(1)式即得 $aH=bH$。上述事实说明，群 G 中的 n 个元素可划分成两两不相交的左陪集之并，每个左陪集都含 m 个元素，因此，m 必是 n 的因数，且指数 $[G:H]$ 恰是 H 在 G 中的左陪集个数。▌

用完全同样的方法可证，G 中 n 个元素可划分成两两不相交的右陪集之并，每个右陪集都含 m 个元素，因此，指数 $[G:H]$ 也是 H 在 G 中的右陪集个数。由此可知 H 在 G 中的左陪集个数与右陪集个数相同。

定理 4·3 设 $K\leqslant H\leqslant G$ 是三个群，且 G 是有限群，则有**指数公式**

$$[G:K]=[G:H][H:K]。$$

事实上，由定理4·2即得

$$[G:K]=\frac{|G|}{|K|}=\frac{|G|}{|H|}\cdot\frac{|H|}{|K|}=[G:H][H:K]$$ ▌

§5 循 环 群

前面已经说过，有限群的阶指的是它所含元素的个数。我们再介绍群中元素的阶这一概念。任一群必有单位元 e，

在整数加群 Z 中，0 是单位元。任何一个非零整数 a 的任意整数倍 na 一定不是 0，除非 $n=0$。但是，并不是任何群都是如此的、例如钟面上的 12 个钟点数关于加法成群。由于规定了 12 点是 0 点，所以凡是 12 的倍数都是 0 点，这个群我们记为①。

$$Z/\langle 12\rangle=\{0,1,2,3,4,5,6,7,8,9,10,11\},$$

0 是单位元，2 的逆元是 10，等等。在这个群中，把 1 相加 12 次得 0，把 2 相加 6 次得 0，对于 5 要相加 12 次才是 0。我们就说，1 是 12 阶元，2 是 6 阶元，5 也是 12 阶元。再考虑由所有 2 阶实可逆阵组成的乘法群 $GL_2(R)$。单位元是单位阵$\begin{pmatrix}1&0\\0&1\end{pmatrix}$。对于$\begin{pmatrix}1&1\\0&1\end{pmatrix}$来说，不管自乘多少次都不会等于$\begin{pmatrix}1&0\\0&1\end{pmatrix}$。但是，把$\begin{pmatrix}0&1\\1&0\end{pmatrix}$自乘 2 次就得到$\begin{pmatrix}1&0\\0&1\end{pmatrix}$。把$\begin{pmatrix}0&1\\-1&-1\end{pmatrix}$自乘 3 次也得到$\begin{pmatrix}1&0\\0&1\end{pmatrix}$。我们说，$\begin{pmatrix}0&1\\1&0\end{pmatrix}$和$\begin{pmatrix}0&1\\-1&-1\end{pmatrix}$分别是 $GL_2(R)$中的 2 阶元和 3 阶元。一般地，若 G 是群，e 是单位元，对任一自然数 n 规定

$$a^n=\underbrace{aa\cdots a}_{n次},\ a^0=e,\ a^{-n}=(a^{-1})^n,$$

则可验证**指数幂法则**成立：对任意整数 m 和 n 有

$$a^na^m=a^{n+m},(a^n)^m=a^{nm}。$$

如果群 G 的运算是加法，则指数幂法则就成为倍数法则

$$na=\underbrace{a+a+\cdots+a}_{n次},\ 0\cdot a=0,\ (-n)a=-(na),$$

---

① 关于 $Z/\langle n\rangle$ 的一般定义见第 47 页

$$na+ma=(n+m)a,\ m(na)=(mn)a,$$

在 $0\cdot a=0$ 中第一个 0 是整数零，第二个 0 是加群中的单位元。对 $a\in G$，使 $a^n=e$ 成立的最小自然数 n 称为 a 的阶，并称 a 是有限阶元。如果只有当 $n=0$ 时才有 $a^n=e$，则称 a 是无限阶元。易见，单位元本身必是 1 阶元。对于加法群来说，$a^n=e$ 指的是 $na=0$。整数加群中任一非零数都是无限阶元。在$GL_2(R)$中，$\begin{pmatrix}1&0\\0&-1\end{pmatrix}$是 2 阶元，$\begin{pmatrix}0&1\\-1&0\end{pmatrix}$是 4 阶元，$\begin{pmatrix}1&1\\0&1\end{pmatrix}$是无限阶元。关于元素的阶有一个常用性质需要证明，即若 a 是 n 阶元，则 $a^n=e, a^{2n}=(a^n)^2=e^2=e,\cdots\cdots$，对任意整数 p 必有 $a^{pn}=(a^n)^p=e$。反过来，若某一个整数 m 使 $a^m=e$，则可证必有 $n|m$（这个记号表示 n 整除 m）。事实上，用整数的带余除法可得 $m=pn+r$，这里 p 和 r 都是整数，且 $0\leqslant r<n$，则 $e=a^m=(a^n)^pa^r=a^r$，但 n 是使 $a^n=e$ 成立的最小自然数，于是由 $0\leqslant r<n$ 知必有 $r=0$，故 $m=pn$。此外，运用拉格朗日定理还可证明一个有趣而且重要的结论，任一有限群 G 中的任一元素 a 必是有限阶元，而且 a 的阶必整除 G 的阶。事实上，如果 a 是无限阶元，则由封闭性知，G 中必包含以下无限个元素

$$\cdots\cdots a^{-3},a^{-2},a^{-1},e,a,a^2,a^3,\cdots\cdots$$

这与 G 是有限群的假设矛盾，所以 a 是有限阶元。设 a 的阶是 n，则 $H=\{e,a,a^2,\cdots,a^{n-1}\}$ 就是 G 的 n 阶子群，于是据拉格朗日定理知 n 整除 G 的阶。

设 G 是群。如果对任意 $a,b\in G$ 都有 $ab=ba$，则称 G 是**交换群**。4 次对称群 S_4 不是交换群，因为$(1\ 2)(1\ 3)=(1\ 2\ 3)$，$(1\ 3)(1\ 2)=(1\ 3\ 2)$。在 S_4 中取出以下 4 个元素

$$(1),(12)(34),(13)(24),(14)(23),$$

容易验证它们组成 S_4 的一个子群，而且是交换群。**这个群比较重要**，我们特地给它取一个名称，称为克莱因(Klein)四元群，记为 $K_4=\{(1),(12)(34),(13)(24),(14)(23)\}$。

我们再把范围缩小一些，考虑一种特殊的交换群——循环群，它在伽罗瓦理论中起着重要的作用，人们将它的结构已经完全搞清楚。我们还是从整数加群 Z 谈起吧。因为 $1\in Z$，$-1\in Z$，任一整数 n 都是 1 或 -1 的正倍数，例如，$5=5\cdot1$，$0=0\cdot1$，$-6=6\cdot(-1)$，所以只要从 1 出发，先得到逆元 -1，然后对 1 或 -1 作适当多次的加法就可得到任一整数。我们就说整数加群 Z 是由一个数 1 生成的循环群，并用符号 $\langle 1\rangle$ 表示：$Z=\langle 1\rangle$。这里，尖括号表示用群的加法运算生成，包括求逆元和逆元相加。尖括号中的元素 1 称为此循环群的一个生成元。用同样方法可证 $Z=\langle -1\rangle$。因此，同一个循环群的生成元不是唯一的。循环群的一般定义为

定义 5·1　若群 G 中的每个元素都是 G 中某个固定元素 a 的整数方幂 a^n，则称 G 是由 a 生成的循环群，记为 $G=\langle a\rangle$。此时，称 a 是 G 的一个生成元。由无限阶元生成的循环群称为无限循环群。否则，称为有限阶循环群。

当然，这里所说的整数方幂是对乘法运算而言的。如果是加法运算，那就是整数倍数 na。根据这个定义，如果循环群 $G=\langle a\rangle$ 的阶是 n，那么 G 中恰有 n 个元素，作为生成元的 a 必定是一个 n 阶元。反之，n 阶循环群中的任一 n 阶元必能生成 n 个互异元，所以它必是生成元。特别地，若 p 是素数，G 是 p 阶群，据拉格朗日定理，G 中任一非单位元素 a 的阶必整除 p，但 p 是素数，a 必是 p 阶元。所以素数阶群必是循环群。它是交换群，没有真子群，而且任一非单位元都是生

成元。这说明素数 p 阶群必有 $p-1$ 个生成元。容易看出，无限循环群 $\langle a\rangle$ 有且仅有两个生成元 a 和 a^{-1}。介于这两种极端情况之间，我们可以证明，在任一 n 阶循环群 $\langle a\rangle$ 中，某个元素 a^k 是生成元当且仅当 k 与 n 互素：$(k,n)=1$（意即 k 和 n 的最高公因数是 1）。为此，只要证明 a^k 是 n 阶元当且仅当 $(k,n)=1$。设 $(k,n)=1$，a^k 的阶是 r，则 $a^{kr}=e$。但 a 的阶是 n，必有 $n|kr$。再由 $(k,n)=1$，知 $n|r$。另一方面，根据拉格朗日定理知，a^k 的阶 r 必整除群的阶 n，即 $r|n$。由于 r 和 n 都是自然数，故必有 $r=n$，即 a^k 是 n 阶元。反之，设 $(k,n)=d\neq 1$，可设 $k=dk'$，$n=dn'$，必有 $k'<k$，$n'<n$，于是，由 $a^{kn'}=a^{k'dn'}=(a^n)^{k'}=e$ 知，a^k 的阶不会超过 n'，所以它不是 n 阶元。这样，我们就证明了 n 阶循环群中生成元的个数恰好就是不超过 n、且与 n 互素的自然数个数。这个数通常用 $\varphi(n)$ 表示①，称为**欧拉函数**。特别地，对素数 p，有 $\varphi(p)=p-1$。例如，4阶循环乘群 $\{1,\sqrt{-1},-1,-\sqrt{-1}\}$ 有两个生成元：$\sqrt{-1}$ 和 $-\sqrt{-1}$，$\varphi(4)=2$。12阶循环加群 $Z/\langle 12\rangle$ 的生成元为 1,5,7,11，$\varphi(12)=4$。7 阶循环加群 $Z/\langle 7\rangle$ 的生成元有六个：1,2,3,4,5,6，$\varphi(7)=6$。

关于循环群，我们还要介绍另一个重要的结果。

定理 5·1　设 $G=\langle a\rangle$ 是循环群（有限或无限），则 G 的任一子群 H 必是循环群 $\langle a^m\rangle$，这里 m 是某个整数。特别地，若 $|G|=n$，则 m 必整除 n，且 $\langle a^m\rangle$ 是 G 唯一的 n/m 阶子群。

证　若 $H=\{e\}$，则一切结论自然成立。设 $H\neq\{e\}$。取

① 设自然数 n 的素数分解式为 $n=q_1^{l_1}q_2^{l_2}\cdots q_s^{l_s}$，则

$$\varphi(n)=n\cdot\prod_{i=1}^{s}\left(1-\frac{1}{q_i}\right).$$

出 H 中具有最小自然数方幂的元素 a^m，它是唯一确定的，这只要考察$a, a^2, a^3, \cdots$，其中第一个落入 H 中的元素a^m即为所求。任取$a^l \in H$。由整数的带余除法，可设 $l=pm+r$，p 和 r 是整数，且$0 \leqslant r < m$，则有$a^l=(a^m)^p \cdot a^r$，但已知$a^l, a^m \in H$，H 是群，所以必有 $a^r=((a^m)^p)^{-1}a^l \in H$。再据 m 的"最小性"知 $r=0$，故 $a^l=(a^m)^p$。这说明 H 中任一元素都是 a^m 的方幂，所以 $H=\langle a^m \rangle$。

如果$\langle a \rangle$是无限循环群，则$\langle a \rangle$中不存在有限阶元，所以$\langle a^m \rangle$也是无限循环群。如果$\langle a \rangle$是 n 阶循环群

$$\langle a \rangle=\{e, a, a^2, \cdots, a^{n-1}\},\ a^n=e,$$

$H=\langle a^m \rangle$是它的某个子群。设 $n=pm+r$，$0 \leqslant r < m$，则$e=a^n=(a^m)^p \cdot a^r$。因为 $a^m \in H$，所以 $a^r \in H$。由 m 的最小性知 $r=0$，即 $n=pm$，所以必有 $m|n$，而且

$$H=\langle a^m \rangle=\{e, a^m, a^{2m}, \cdots, a^{(p-1)m}\}$$

是 $\langle a \rangle$ 的 $p=\frac{n}{m}$阶子群。现再证对确定的 $p=\frac{n}{m}$来说，$\langle a \rangle$的 p 阶子群是唯一的。设 K 是$\langle a \rangle$的任一 p 阶子群，这里 $p=n/m$。根据上面证得的结论，这个子群必是某个$\langle a^{m'} \rangle$，m' 整除 n。可设 $n=p'm'$，且

$$K=\langle a^{m'} \rangle=\{e, a^{m'}, a^{2m'}, \cdots, a^{(p'-1)m'}\},$$

但它显然是 p' 阶群，所以必有$p'=p$。再由 $n=pm=p'm'$ 知 $m'=m$。所以这个 K 就是$\langle a^m \rangle$，这里 $m=n/p$。▌

例如，设$\langle a \rangle$是 12 阶循环群，$a^{12}=e$。因为 3 是 12 的一个因子，所以存在唯一的 4 阶子群

$$\langle a^3 \rangle=\{e, a^3, a^6, a^9\}.$$

又如，在 n 次对称群 S_n 中，任取一个 n- 轮换 σ，不妨以 $\sigma=(1\,2\,3\cdots n)$为例。由计算可知 σ 是 n 阶元，所以

$$\langle\sigma\rangle=\{(1),\sigma,\sigma^2,\cdots,\sigma^{n-1}\}$$

是 S_n 的一个 n 阶循环子群．反过来，S_n 的任一 n 阶循环子群 H，必由一个 n 阶元 σ 生成。但是，这个 σ 未必是某个 n-轮换 $\sigma=(i_1i_2\cdots i_n)$。例如，在 S_{12} 中，$\sigma=(123)(4567)$是一个12 阶元，它生成一个12 阶循环子群$\langle\sigma\rangle$，但 σ 却不是一个12-轮换。

§6 正规子群与商群

在群论中还有一个重要内容，就是如何把一个较大的群变为较小的群，或把结构较复杂的群变为较简单的群。为此，我们要引入群的正规子群和商群概念，也就是要考虑两个群怎样相除了！我们先举一个最简单的例子。考虑整数加群 Z。显然，偶数加群 E 是它的子群。如果我们只关心某整数是奇数还是偶数，而並不关心它的确切数值，那末可以认为偶数之间并无差别，可用符号 0 表示；奇数之间也无差别，可用 1 表示。因为偶数加奇数是奇数，两个偶数之和以及两个奇数之和都是偶数，所以在由此产生的两元集合 $\{0,1\}$ 上可规定一种运算：$0+0=0$，$1+1=0$，$0+1=1+0=1$。易见，它是一个 2阶加群，可以把它看成是 Z 除以 E 所得的商群。这个群很小而且结构非常简单。遗憾的是，并不是任意两个群都可以相除，能够用来除别的群的那个群必须是前者的正规子群——这是一种满足某个特定条件的子群。由于在讨论可解群时，

正规子群是必不可少的概念，所以我们要先将它介绍一下。

设 G 是群，H 是 G 的子群。任取 $h\in H$，$g\in G$。由于 G 不一定是交换群，所以 $g^{-1}hg$ 未必等于 h，它甚至未必属于 H。例如，考虑 S_3 的子群 $H=\{(1),(12)\}$。取 $(13)\in S_3$，得到 $(13)^{-1}(12)(13)=(23)$，它不属于 H。

定义 6·1 设 H 是群 G 的子群。如果对任意 $h\in H$，$g\in G$，必有 $g^{-1}hg\in H$，则称 H 是 G 的**正规子群**，记为$H\lhd G$，也可记为 $G\rhd H$。

注意，这里横着放的等腰三角形具有方向性，它的顶角总指向子群。显然，交换群的任一子群必是正规子群。

设 H 是群 G 的任一子群。任意取定某个 $g\in G$。考虑G的如下子集

$$\overline{H}=\{g^{-1}hg\mid h\in H\},$$

我们把它记作 $g^{-1}Hg$，这是一个集合记号。应用判别子群的定理4·1，可以验证 $\overline{H}$ 也是 G 的子群，称为 H 在 G 中的一个**共轭子群**。对 $h\in H,g\in G$，元素 $g^{-1}hg$ 称为 h 在 G 中的一个**共轭元**。事实上，对$g^{-1}h_1g$，$g^{-1}h_2g\in\overline{H}$，有

$$(g^{-1}h_1g)(g^{-1}h_2g)=g^{-1}(h_1h_2)g\in\overline{H},$$

$$(g^{-1}h_1g)^{-1}=g^{-1}h_1^{-1}g\in\overline{H}。$$

特别地，如果 H 是 G 的正规子群，一方面，由正规子群的定义立刻得到 $\overline{H}\subseteq H$；另一方面，任取 $h\in H$，仍由正规子群的定义知

$$ghg^{-1}=(g^{-1})^{-1}hg^{-1}=h_1\in H,$$

所以，$h=g^{-1}h_1g\in\overline{H}$，这又说明 $H\subseteq\overline{H}$，于是 $\overline{H}=H$，即$g^{-1}Hg$

$=H$, $\forall g\in G$。这说明 G 的任一正规子群 H 的任一共轭子群必是 H 本身，所以正规子群又称为**自共轭子群**。反之，若 H 是 G 的某个子群，且对任意 $g\in G$ 都有 $g^{-1}Hg=H$，则对任一 $h\in H$, $g\in G$, 必有 $g^{-1}hg\in H$，所以 H 必是 G 的正规子群。于是得到正规子群的第一个性质：

(1)群 G 的子群 H 是正规子群 $\Longleftrightarrow g^{-1}Hg=H$, $\forall g\in G$。

根据集合相等的定义不难证明，$g^{-1}Hg=H\Longleftrightarrow Hg=gH$，即包含 g 的右陪集与左陪集相同，所以得到正规子群的又一性质：

(2)群 G 的子群 H 是正规子群 $\Longleftrightarrow Hg=gH$, $\forall g\in G$。

这就是说，对于正规子群的陪集来说，根本不必区分左陪集和右陪集，可以统称为陪集。利用这个事实我们还可证明正规子群的第三个性质：

(3) G 的指数为 2 的子群 H 必是正规子群。

事实上，根据指数的定义可知，集合 G 既是仅有的两个左陪集 H 与 $gH(g\notin H)$ 的并集，又是仅有的两个右陪集 H 和 Hg 的并集，且 H 与 gH 不相交，H 与 Hg 也不相交，$gH\neq H$，所以必有 $gH=Hg$。这个等式对任意 $g\in H$ 都成立，所以 H 是 G 的正规子群。

我们要强调指出，正规性没有传递性。确切地说，就是

(4)若 $H\leqslant K\leqslant G$ 是三个群。如果 $H\lhd G$，则 $H\lhd K$，但未必有 $K\lhd G$。如果 $H\lhd K$, $K\lhd G$，则未必有 $H\lhd G$。事实上，因为 $H\lhd G$，所以对任何 $h\in H$ 和 $g\in G$ 必有 $g^{-1}hg\in H$，而 $K\subseteq G$，当然，对任一 $k\in K$ 有 $k^{-1}hk\in H$，所以 $H\lhd K$。要说明正规性没有传递性，只要举出一个反例就足够了。例如，考虑 4 次交错群 A_4 的如下两个子群

$K_4=\{(1),(12)(34),(13)(24),(14)(23)\}$,

$$H=\{(1),(12)(34)\}.$$

因为 $[K_4:H]=2$，所以 $H\lhd K_4$。可以验证

$$A_4=\{K_4,(123),(124),(134),(234),(132),$$
$$(142),(143),(243)\}$$

中任一元素确定的 K_4 的左、右陪集都是相同的，例如，

$$(123)\cdot K_4=\{(123),(243),(142),(134)\}=K_4\cdot(123)$$

等等，所以 $K_4\lhd A_4$。但是由

$$(123)\cdot H=\{(123),(243)\},\ H\cdot(123)=\{(123),(134)\}$$

不相等知，H 不是 A_4 的正规子群。

现在我们将要说明，对于群的正规子群就可以作除法。设 N 是群 G 的正规子群，把 N 在 G 中的陪集全体记为

$$G/N=\{aN\,|\,a\in G\}.$$

注意，集合 G/N 的元素是陪集，也即 G/N 是由若干个集合组成的集合。在 G/N 中规定如下运算

$$(aN)(bN)=abN,\ \forall a,b\in G.$$

说到这里，必须要弄清楚一件事。我们所说的运算必须是单值运算，即对于任意两个确定的元素，其运算结果只能有一个，正如 $1+2$ 等于 3 而不能是其它任何数一样。但是现在的运算对象是一些集合，而且存在不同的元素 a 和 a' 使 $aN=a'N$，这只要保证 $a^{-1}a'\in N$ 就可以了。同理，也存在不同的 b 和 b' 使 $bN=b'N$。于是根据 G/N 中乘法的定义又有

$$(aN)(bN)=(a'N)(b'N)=a'b'N.$$

那末自然要问，是否必有 $abN=a'b'N$ 呢？其回答是，只要 N 是 G 的正规子群，上述等式必定成立①。事实上，据 $aN=a'N$，$bN=b'N$，可设 $a'=ah_1$，$b'=bh_2$，$h_1,h_2\in N$，所以 $a'b'=ah_1bh_2$。但由 $Nb=bN$ 可知对这个 $h_1\in N$，必存在 $h_3\in N$ 使 $h_1b=bh_3$，所以 $a'b'=abh_3h_2\in abN$。这说明 abN 和 $a'b'N$ 含有公共元素 $a'b'$，所以必有 $abN=a'b'N$。现在可以得到

定理 6·1　设 N 是群 G 的正规子群，则

$$G/N=\{aN\mid a\in G\}$$

关于由 $(aN)(bN)=abN$ 定义的乘法成群，称为 G 模 N 的商群。特别当 G 是有限群时，商群的阶

$$|G/N|=[G:N]=|G|/|N|。$$

证　逐一验证 G/N 成群的四个条件

(1)封闭性。由 $ab\in G$ 知 $(aN)(bN)=abN\in G/N$。

(2)结合律。由 $(ab)c=a(bc)$ 知

$$((aN)(bN))(cN)=(abN)(cN)=(ab)cN,$$

$$(aN)((bN)(cN))=(aN)(bcN)=a(bc)N,$$

两者相等。

(3) N 是 G/N 中的单位元。事实上，利用 $N=eN$ 知

$$N(aN)=(ea)N=aN,$$

$$(aN)N=(ae)N=aN,$$

对任一 $a\in G$ 成立，这里 e 是群 G 的单位元。

(4) aN 在 G/N 中的逆元是 $a^{-1}N$：

---

① 进一步可证，若 N 不是 G 的正规子群，则此等式一定不成立，所以，N的正规性仅仅用来保证陪集乘法的单值性。

$$(aN)(a^{-1}N)=(aa^{-1})N=N,$$

$$(a^{-1}N)(aN)=(a^{-1}a)N=N。$$

所以 G/N 成群。如果 G 是有限群，则 N 在 G 中的陪集个数就是指数 $[G:N]$，所以 $|G/N|=|G|/|N|$。∎

例如，整数加群 Z 是交换群，它的任一子群必是正规子群，偶数加群 E 在 Z 中的陪集只有两个，一个就是 E，它是偶数全体，另一个就是 $a+E$，这里 a 是任一奇数，$a+E$ 就是奇数全体，所以 Z 模 E 的商群是 2 阶加群，记为 $Z/\langle 2\rangle=\{0,1\}$，$2=0$，这里 $\langle 2\rangle$ 是由 2 生成的循环加群，也即偶数加群 E。凡是被 3 整除的整数全体也是 Z 的子群，它就是由 3 生成的循环加群 $\langle 3\rangle$。Z 模 $\langle 3\rangle$ 的商群就是 3 阶加群 $Z/\langle 3\rangle=\{0,1,2\}$，这里规定 $1+2=0$，$2+2=1$。一般地，对任意取定的自然数 n，凡被 n 整除的整数全体成 Z 的子群 $\langle n\rangle$，它是 n 阶循环加群，Z 模 $\langle n\rangle$ 的商群就是 n 阶加群

$$Z/\langle n\rangle=\{0,1,2,\cdots,n-1\},$$

这里规定，加到 n 时就得 0。例如，钟面上的钟点数成加法群 $Z/\langle 12\rangle$，每周中的 7 天成 $Z/\langle 7\rangle$，它们都是商群。

在这里还可发现一个有趣的事实：对于无限循环群 $Z=\langle 1\rangle$，前已证明它的子群必是无限循环群 $\langle n\rangle$，n 是这个子群中的最小自然数。现在则发现 $Z/\langle n\rangle$ 是 n 阶循环群！实际上，这对任何循环群都是成立的。

定理 6·2 设 $G=\langle a\rangle$ 是任一循环群，$N=\langle a^m\rangle$ 是 G 的子群，m 是 N 中元素的最小自然数方幂，则 G/N 必是 m 阶循环群 $\langle aN\rangle$。

证 首先证明，由 G 的生成元 a 所确定的陪集 aN 恰是

m 阶元。事实上，由 $a^m \in N$，知 $(aN)^m = a^m N = N$，而 N 是 G/N 的单位元。对任一满足于 $1 \leqslant m' < m$ 的 m'，有 $(aN)^{m'} = a^{m'} N \neq N$。因为否则的话，必有 $a^{m'} \in N$，与 m 的最小性矛盾。所以 aN 恰是群 G/N 中的 m 阶元。其次，任取 $gN \in G/N$。因为 $G = \langle a \rangle$，可设 $g = a^l$，l 是某一整数。设 $l = pm + r$，$0 \leqslant r < m$，则

$$gN = a^l N = (aN)^l = (aN)^{mp} \cdot (aN)^r$$
$$= N(aN)^r = (aN)^r。$$

这说明 gN 可表成 aN 的方幂，所以 $G/N = \langle aN \rangle$ 为 m 阶循环群。▌

把这个定理应用到 Z 上（运算要换成加法），就可得知 $Z/\langle n \rangle$ 是 n 阶循环群。

§7 同态与同构

在 §2 的开头，我们曾经提到过，人们将群论作为一种工具，采用抽象的观点和逻辑推理的方法，可以统一处理一些代数系统。这些代数系统在形式上可以完全不同，但从群论观点来看，却没有结构上的差别。这就是同构的概念，其含义就是有相同的代数结构。我们还是举一个实例来说明问题吧！实数加群 $(R, +)$ 和正实数乘群 $(R^+, \cdot)$ 是不同的两个群。如果我们取定某个正实数 $a \neq 1$，则利用对数性质知，对任意两个正实数 r_1 和 r_2，有等式

$$\log_a r_1 r_2 = \log_a r_1 + \log_a r_2,$$

这就是说，若要计算两个正实数的乘积，可先算出它们的对数

之和，再用反对数表查出乘积值。换句话说，可把正实数的乘法化为实数的加法。这件事暗示着我们，在群$(R^+,\cdot)$与$(R,+)$之间必定有着某种本质上的联系，这个联系就是$(R^+,\cdot)$到$(R,+)$的取对数映射：$r^\varphi=\log_a r$，它有性质

$$(r_1r_2)^\varphi=r_1^\varphi+r_2^\varphi,$$

即乘积的对数等于对数之和。现在我们就来讨论具有这种性质的映射。

设G和$\overline{G}$是两个群，各有各的运算，为了书写简洁起见，干脆都不明显写出。G中元素用a，b等表示，$\overline{G}$中元素用$\overline{a}$，$\overline{b}$等表示，ab表示按G中运算求值，$\overline{a}\,\overline{b}$表示按$\overline{G}$中运算求值。

定义 7·1 设φ是群G到群$\overline{G}$的映射，如果它满足条件

$$(ab)^\varphi=a^\varphi b^\varphi,\quad \forall a,b\in G,$$

则称φ是G到$\overline{G}$的**同态映射**。如果同态映射φ又是单射，则称为**同构映射**。

上述这一条件常被说成φ保持群的运算。无论是同态映射还是同构映射，都未必要是满射。如果在群G和$\overline{G}$之间至少存在一个G到$\overline{G}$的同态满射(或同构满射)，则称G和$\overline{G}$是同态的(或同构的)，记为$G\overset{\varphi}{\sim}\overline{G}$ (或$G\overset{\varphi}{\cong}\overline{G}$)。有时并不需要把$\varphi$明显写出，就写成$G\sim\overline{G}$ (或$G\cong\overline{G}$)。例如，$(R^+,\cdot)\cong(R,+)$，其中同构映射可取为$\varphi:r\to\log_a r$，a是某个取定的不等于1的正实数。

一般说来，如果$G\sim\overline{G}$，则未必有$\overline{G}\sim G$。例如，G是元素个数$\geqslant2$的任意一群，$\overline{G}$是某个单位元群$\{\overline{e}\}$，则$\varphi:a\to\overline{e}$，$\forall a\in G$显然是G到$\overline{G}$的同态满射，然而由$|G|\geqslant2$知，决不存

在 $\overline{G}$ 到 G 的同态满射(单值性!),所以同态关系是单方向、不可逆的,"两个同态的群"这句话的含义是不确切的。如果,$G\overset{\varphi}{\cong}\overline{G}$,则 φ 是 G 到 $\overline{G}$ 的双射,对任一 $\overline{a}\in\overline{G}$,必存在唯一的 $a\in G$ 使 $a^{\varphi}=\overline{a}$,所以这个 φ 也确定了 $\overline{G}$ 到 G 的双射

$$\varphi^{-1}: \overline{a}\to a,\ \forall\overline{a}\in\overline{G},\ \text{这里}\overline{a}=a^{\varphi}.$$

进一步可证 φ^{-1} 是 $\overline{G}$ 到 G 的同构满射。事实上,对 $\overline{a}$, $\overline{b}\in\overline{G}$,存在 a, $b\in G$,使 $a^{\varphi}=\overline{a}$, $b^{\varphi}=\overline{b}$, 则 $\overline{a}^{\varphi^{-1}}=a$, $\overline{b}^{\varphi^{-1}}=b$,于是由 $(ab)^{\varphi}=a^{\varphi}b^{\varphi}=\overline{a}\,\overline{b}$ 得

$$(\overline{a}\overline{b})^{\varphi^{-1}}=ab=\overline{a}^{\varphi^{-1}}\overline{b}^{\varphi^{-1}},$$

所以必有 $\overline{G}\overset{\varphi^{-1}}{\cong}G$。这说明同构关系是可逆的,"两个同构的群"这句话的含义是确切的。

同态满射有如下两个简单性质。设 $G\overset{\varphi}{\sim}\overline{G}$, e 是 G 的单位元,则对任意 $a\in G$, 有 $ea=ae=a$。考虑在同态映射 φ 之下的象,就有 $e^{\varphi}a^{\varphi}=a^{\varphi}e^{\varphi}=a^{\varphi}$。因为 φ 是满射, a^{φ} 可取遍 $\overline{G}$ 中所有元素,所以 e^{φ} 必是 $\overline{G}$ 的单位元。同理,若 b 是 $a\in G$ 在 G 中的逆元: $ab=ba=e$, 则由 $a^{\varphi}b^{\varphi}=b^{\varphi}a^{\varphi}=e^{\varphi}$ 知 b^{φ} 是 $a^{\varphi}\in\overline{G}$ 在 $\overline{G}$ 中的逆元。这一事实常用关系式 $(a^{-1})^{\varphi}=(a^{\varphi})^{-1}$ 表示,这里,两个求逆号分别在 G 和 $\overline{G}$ 中求逆。所以同态满射必把单位元变为单位元,逆元变为逆元。

读者可以根据群同构的定义证明,任一无限循环群 $\langle a\rangle$ 必同构于整数加群,同构满射可取为 $\varphi: a^{k}\to k$, $\forall k\in Z$; 任一 n 阶循环群 $\langle a\rangle=\{e,a,a^{2},\cdots a^{n-1}\}$, $a^{n}=e$ 必同构于 n 阶加群 $Z/\langle n\rangle=\{0,1,2,\cdots,n-1\}$, $n=0$。因为同构满射是一一对应,所以两个同构的有限群所含的元素个数必定相同。但对无限群来说,一个群完全可能同它的一个真子群同构。例如,整数

加群与偶数加群是同构的，同构满射可取为 $n\to 2n$，$\forall n\in Z$。

最后，我们介绍应用广泛的同态定理，它也是抽象代数学中的基本定理之一。

定理 7·1 （同态定理）

(1)设 N 是群 G 的正规子群，则 $G\sim G/N$，即群 G 的任一商群必是 G 的同态象。

(2)设群 $G\overset{\varphi}{\sim}\overline{G}$，$\bar{e}$ 是群 $\overline{G}$ 的单位元，则 $\bar{e}$ 在 φ 之下的原象全体

$$K=\{k\mid k\in G,k^{\varphi}=\bar{e}\}$$

必是 G 的正规子群，称为同态 φ 的核，且 $G/K\cong\overline{G}$，即群 G 的任一同态象 $\overline{G}$ 必同构于 G 的某个商群 G/K，这里 K 就是该同态的核。

证 (1)由 $(aN)(bN)=abN$ 知

$$\nu: a\to aN,\quad \forall a\in G$$

是 G 到 G/N 的同态满射，所以 $G\overset{\nu}{\sim}G/N$。称这种 ν 为**自然同态**。

(2)任取 $k_1,k_2\in K$，则由

$$(k_1k_2)^{\varphi}=k_1^{\varphi}k_2^{\varphi}=\bar{e},\quad (k_1^{-1})^{\varphi}=(k_1^{\varphi})^{-1}=\bar{e}$$

知 $k_1k_2\in K$，$k_1^{-1}\in K$，所以 $K\leqslant G$。任取 $k\in K$，$g\in G$，则由

$$(g^{-1}kg)^{\varphi}=(g^{\varphi})^{-1}k^{\varphi}g^{\varphi}=(g^{\varphi})^{-1}g^{\varphi}=\bar{e}$$

知 $g^{-1}kg\in K$，所以 $K\lhd G$。任取 $a\in G$，设 $a^{\varphi}=\bar{a}$。考虑 G/K 到 $\overline{G}$ 的映射

$$\varphi^{*}: aK\to\bar{a},\ \forall aK\in G/K，这里\ \bar{a}=a^{\varphi}。$$

因为 φ 是满射，所以 φ^* 也是满射。因为

$$aK=bK \Longleftrightarrow b^{-1}a\in K \Longleftrightarrow (b^{-1}a)^{\varphi}=(b^{\varphi})^{-1}a^{\varphi}=\bar{e}$$

$$\Longleftrightarrow a^{\varphi}=b^{\varphi} \Longleftrightarrow \bar{a}=\bar{b},$$

所以 φ^* 是单值映射和单射。最后，由

$$(aK)(bK)=abK \xrightarrow{\varphi^*} \overline{ab}=(ab)^{\varphi}=a^{\varphi}b^{\varphi}=\bar{a}\bar{b}$$

知 φ^* 的确是同构满射，所以

$$G/K \overset{\varphi^*}{\cong} \bar{G}。\blacksquare$$

例如，$n(\geqslant 2)$ 次对称群 S_n 同态于 2 阶乘法群 $G=\{1,-1\}$，G 中乘法就是数的乘法，同态满射可取为

$$\varphi:\sigma \longrightarrow \begin{cases} 1, & 若\ \sigma\ 是偶置换, \\ -1, & 若\ \sigma\ 是奇置换. \end{cases}$$

这个同态的核就是 n 次交错群 A_n，故

$$S_n/A_n \cong \{1,-1\}.$$

所以 $[S_n:A_n]=2$，$A_n \lhd S_n$，且

$$|A_n|=\frac{1}{2}|S_n|=\frac{1}{2}n! \qquad n\geqslant 2。$$

又如，由行列式乘法规则 $\det(AB)=\det A\cdot\det B$ 知

$$\varphi: A\to \det A$$

是 $GL_n(R)$ 到 R^* 的同态满射，其核就是 $SL_n(R)$，它是 $GL_n(R)$ 的正规子群，且

$$GL_n(R)/SL_n(R)\cong R^*,$$

这里 R^* 是非零实数乘法群。

§8 可 解 群

在第四章中我们将要说明，一个代数方程能否用根号求解，归之于它所对应的某个群是否是一个"可解群"，因此，我们专门列一节向读者介绍什么是可解群。

还是从4次对称群S_4谈起吧。S_4是24阶群，A_4是它的12阶子群，所以$A_4 \lhd S_4$。前已提到克莱因四元群

$$K_4=\{(1),(12)(34),(13)(24),(14)(23)\}$$

是A_4的正规子群。单位元群$\{(1)\}$当然是K_4的正规子群。这样，我们就得到了一个子群有限长序列：

$$S_4 \rhd A_4 \rhd K_4 \rhd 1,$$

这里的1表示单位元群$\{(1)\}$。后一个群是前一群的正规子群。我们把这一序列称为S_4的一个正规群列．一般地，我们有

定义 8·1 群G的如下子群的有限长序列

$$G=G_0 \rhd G_1 \rhd \cdots\cdots \rhd G_{r-1} \rhd G_r=1 \qquad (1)$$

称为G的一个正规群列。相邻两群的商群G_i/G_{i+1}称为这一正规群列的因子群($i=0,1,2,\cdots,r-1$)。1表示G的单位元群。

注意，这里只要求G_{i+1}是G_i的正规子群，它足以保证G_i/G_{i+1}成群，并不要求G_i是其它$G_j(j<i)$的正规子群(正规性没有传递性)。易见，任意一个群G必有正规群列。例如$G \rhd 1$就是一个正规群列。然而正规群列未必是唯一的。不同的正规群列当然有不同的因子群组。

定义 8·2 称群 G 是可解群，如果存在某个正规群列，它的每个因子群都是交换群。

因为交换群的子群和商群仍是交换群，所以任意交换群必是可解群。例如，$S_2=\{(1),(12)\}$必是可解群。

请读者注意定义中的"存在某个"四个字，这就是说，对于可解群来说，不能保证它的任一正规群列的因子群都是交换群。例如，$S_3 \rhd A_3 \rhd 1$ 中，S_3/A_3 和 $A_3/1$ 都是交换群，所以 S_3 是可解群。但对正规群列 $S_3 \rhd 1$ 来说，因子群 $S_3/1$ 却不是交换群。前已说过，S_4 有正规群列

$$S_4 \rhd A_4 \rhd K_4 \rhd 1,$$

前两个因子群的阶依次为 2 和 3，都是素数阶群，必是交换群。可以直接验证 K_4 是交换群，所以 S_4 也是可解群。那末，S_5 是否是可解群？是否存在 S_5 的某个正规群列，其每个因子群都是交换群？出乎人们的意料，S_5 竟不是可解群！ 4 与 5 仅相差 1，但两数之间却隔着一条不可逾越的鸿沟！S_4与S_5有着本质的差别。但是，从另一角度来看，幸亏发现了这个差别，才导致高次代数方程根号求解问题的彻底解决。不过 S_5 不是可解群这一事实，不是三言两语就能讲清楚的。为此首先还要引进群的换位子群的概念。

设 G 是任一群。任取 a，$b \in G$，必可确定 G 中一个特殊元素$a^{-1}b^{-1}ab$，通常记为

$$[a,b]=a^{-1}b^{-1}ab,$$

我们把它称为 a 与 b 的换位子。请注意，整个方括号仅表示一个元素。为什么要取这个怪名字呢？由换位子的定义式知，$ba[a,b]=ab$，这说明换位子这个元素右乘 ba 得到的是 ab，

这不是把 b 和 a 换了一个位置吗？a 与 b 的换位子是 $[a,b]=a^{-1}b^{-1}ab$，b 与 a 的换位子是 $[b,a]=b^{-1}a^{-1}ba$，这两者未必相同，而它们的乘积 $[a,b][b,a]=e$ 是 G 中单位元，所以 $[a,b]^{-1}=[b,a]$。易见，G 中两个元素 a 与 b 可交换 $ab=ba$ 当且仅当 $[a,b]=e$。进一步，一个群 G 是交换群当且仅当 G 中任意两个元素的换位子都是单位元 e。这个事实在定理8·1中要用到。一般地说，两个换位子的乘积未必是换位子，即对 $a,b,c,d\in G$ 来说，未必存在 $x,y\in G$ 使得 $[a,b][c,d]=[x,y]$。因此，换位子集合不满足封闭性条件。但是，可以证明，G 的如下子集

$$D(G)=\{G\text{中有限个换位子相乘所得的乘积}\}$$

必是 G 的正规子群。事实上，两个有限个换位子的乘积相乘得到的仍是有限个换位子的乘积，所以 $D(G)$ 满足封闭性条件。因为 $D(G)$ 是群 G 的子集，结合律自然满足。单位元 $e=[e,e]$ 当然是换位子。再由 $[a,b]^{-1}=[b,a]$ 知换位子之逆仍是换位子，所以有限个换位子乘积的逆元仍是有限个换位子的乘积，仍在 $D(G)$ 中。这就说明了 $D(G)$ 是 G 的子群。进一步，任取 $g\in G$，$[a,b]\in D(G)$，有

$$\begin{aligned} g^{-1}[a,b]g &= g^{-1}a^{-1}b^{-1}abg \\ &= (g^{-1}ag)^{-1}(g^{-1}bg)^{-1}(g^{-1}ag)(g^{-1}bg) \\ &= [g^{-1}ag, g^{-1}bg], \end{aligned}$$

它仍是一个换位子，所以，任取 $g\in G$，$d=d_1d_2\cdots d_r\in D(G)$（这里每个 d_i 都是换位子），必有

$$g^{-1}dg=(g^{-1}d_1g)(g^{-1}d_2g)\cdots(g^{-1}d_rg),$$

它仍是有限个换位子的乘积，即属于 $D(G)$，所以 $D(G)\lhd G$。

G 的这个正规子群 $D(G)$ 称为 G 的**换位子群**。群 G 的换位子群有以下重要性质：

定理 8·1 设 G 是群，$D(G)$ 是 G 的换位子群，则

(1) $G/D(G)$ 必是交换群；

(2) 若 N 是 G 的使 G/N 是交换群的正规子群，则 $N \supseteq D(G)$。这就是说，群的换位子群是使商群是交换群的最小正规子群。

证 (1)把商群 $G/D(G)$ 中每个元素(陪集)记为

$$\bar{g} = gD(G), \quad g \in G,$$

则据陪集乘法的定义易证，$\bar{g}\bar{h} = \bar{h}\bar{g}$，(因为 $g^{-1}h^{-1}gh \in D(G)$) $\bar{g}^{-1} = \overline{g^{-1}}$，$\forall g$，$h \in G$。于是，$G/D(G)$，中任何一个换位子

$$\bar{g}^{-1}\bar{h}^{-1}\bar{g}\bar{h} = \overline{g^{-1}h^{-1}gh}$$
$$= (g^{-1}h^{-1}gh)D(G) = D(G)$$

(因为 $g^{-1}h^{-1}gh \in D(G)$) 是 $G/D(G)$ 中的单位元 $D(G)$，所以 $G/D(G)$ 是交换群。

(2)任取 g，$h \in G$。由 G/N 是交换群知

$$N = (gN)^{-1}(hN)^{-1}(gN)(hN) = (g^{-1}h^{-1}gh)N,$$

这说明 $g^{-1}h^{-1}gh \in N$，所以 $D(G) \subseteq N$。

本章的主要目标就是要得到如下结果。

定理 8·2 当 $n \geqslant 5$ 时，S_n 不是可解群。

证 如果 $G = S_n$ 是可解群，则存在某个正规群列

$$G = G_0 \triangleright G_1 \triangleright \cdots \triangleright G_{k-1} \triangleright G_k \triangleright \cdots \triangleright G_r = 1,$$

这里 1 表示 G 的单位元群，它由 S_n 中恒等变换构成。每个因子群 G_{k-1}/G_k 都是交换群。现要证明这是不可能的。为此，

我们对 k 用归纳法证明以下事实：当 G_{k-1} 包含 S_n 中所有3-轮换时，G_k 也必定包含 S_n 中所有 3-轮换。这样就决不可能存在是单位元群的 G_r 了，而 r 是有限数. $G_0=S_n$ 当然包含 S_n 中所有 3-轮换. 设 G_{k-1} 包含 S_n 中所有 3-轮换. 在 1 与 n 之间任意取定五个两两互异的自然数 i, j, k, l 和 m（因为 $n\geqslant 5$，这总是办得到的），则

$$\sigma=(i\ l\ j),\quad \tau=(j\ k\ m)\in G_{k-1},$$

因为 G_{k-1}/G_k 是交换群，据定理8·1，$D(G_{k-1})\subseteq G_k$，所以

$$\sigma^{-1}\tau^{-1}\sigma\tau=(j\ l\ i)(m\ k\ j)(i\ l\ j)(j\ k\ m)$$
$$=(i\ j\ k)\in G_k,$$

这就证明了 G_k 也包含了 S_n 中所有 3-轮换. ▌

推论 当 $n\geqslant 5$ 时，A_n 不是可解群。

证 如果 A_n 是可解群，则有因子群都是交换群的正规群列 $A_n\triangleright\cdots\triangleright 1$。在上一节末已证明 S_n/A_n 是 2 阶交换群，所以 $S_n\triangleright A_n\triangleright\cdots\triangleright 1$ 就成了 S_n 的正规群列，其每个因子群都是交换群，于是 S_n 是可解群，这是不可能的，所以 A_n 不是可解群. ▌

最后，还必须解决一个问题：如何判别某个给定的群是可解群？这仍要借助于换位子群。设 G 是群，$D(G)$ 是 G 的换位子群。$D(G)$ 既然是一个群，它也有换位子群，记为 $D^2(G)$，它的元素是有限个形如 $[d_1, d_2]$ 的元素的积，d_1 和 d_2 是 G 中元素的有限个换位子之积。同理，把群 $D^2(G)$ 的换位子群记为 $D^3(G)$，……如此下去可得 G 的如下子群列

$$G\triangleright D(G)\triangleright D^2(G)\triangleright D^3(G)\triangleright\cdots\cdots$$

一般说来，它未必是有限长的序列. 我们把它称为 G 的**换位**

群列。可以证明

定理 8·3　群 G 是可解群 $\Longleftrightarrow$ 存在自然数 k 使 $D^k(G)=1$，这里 1 代表 G 的单位元群。换句话说，群 G 是可解群当且仅当 G 的换位群列有限步终于 1。

证　必要性。设 G 是可解群，则据定义知存在某个正规群列

$$G=G_0\rhd G_1\rhd G_2\rhd\cdots\rhd G_{k-1}\rhd G_k=1,$$

其中每个因子群 G_i/G_{i+1} 都是交换群。于是据定理8·1，依次有

$$G_1\supseteq D(G_0)=D(G),$$

$$G_2\supseteq D(G_1)\supseteq D^2(G),$$

这里，包含关系 $D(G_1)\supseteq D^2(G)$ 是根据以下事实得出的：因为 $D(G)$ 是 G_1 的子群，$D(G)$ 中的换位子必是 G_1 中的换位子，所以 $D^2(G)$ 是 $D(G_1)$ 的子群。类似地有

$$G_3\supseteq D(G_2)\supseteq D^3(G),$$

$$\cdots\cdots$$

$$G_{k-1}\supseteq D(G_{k-2})\supseteq D^{k-1}(G),$$

$$G_k\supseteq D(G_{k-1})\supseteq D^k(G)。$$

但已知 $G_k=1$，所以 $D^k(G)=1$。

充分性。设 $D^k(G)=1$，则 G 有如下正规群列

$$G\rhd D(G)\rhd D^2(G)\rhd\cdots\rhd D^k(G)=1,$$

且由定理8·1知每个因子群 $D^i(G)/D^{i+1}(G)$ 都是交换群（这里 $D^0(G)=G$，$D^1(G)=D(G)$），所以 G 是可解群。▌

推论 可解群的子群和商群必是可解群。

证 (1)若 G 是可解群，可设 $D^k(G)=1$。设 H 是 G 的任一子群。由换位子的定义易见 $D^k(H)\subseteq D^k(G)$。但 $D^k(G)=1$，所以 $D^k(H)=1$，H 是可解群。

(2)若 G/N 是 G 的任一商群。考虑自然同态 $G\overset{\nu}{\sim}G/N$。对任一 $g\in G$，有 $g^\nu=gN=\bar{g}$。用 $G^\nu=G/N$ 表示 G 在 ν 之下的象群。由陪集乘法的定义知，对 g，$h\in G$ 有

$$g^{-1}h^{-1}gh\overset{\nu}{\longrightarrow}(g^{-1}h^{-1}gh)N$$

$$=\overline{g^{-1}h^{-1}gh}=\bar{g}^{-1}\bar{h}^{-1}\bar{g}\bar{h},$$

即 ν 把 G 的换位子映为 G^ν 中的换位子。反之，G^ν 中任一换位子$[\bar{g},\bar{h}]$必是 G 中换位子 $[g,h]$ 在 ν 之下的象，所以ν把 G 的换位子群 $D(G)$ 映为 G^ν的换位子群 $D(G^\nu)$，即

$$D(G)\overset{\nu}{\longrightarrow}D(G^\nu).$$

同理可得

$$D^2(G)\overset{\nu}{\longrightarrow}D^2(G^\nu),$$

......

$$D^k(G)\overset{\nu}{\longrightarrow}D^k(G^\nu).$$

因为同态映射把单位元映为单位元，所以当 $D^k(G)=1$时，必有 $D^k(G^\nu)=1^\nu$，这里 1^ν 是 $G^\nu=G/N$ 的单位元 N。于是证得 G/N 是可解群。▌

在群论中还有一个重要概念，就是单群。每个群 G 都有两个平凡正规子群 $\{e\}$ 和 G。如果某个群 G 除了这两个平凡正规子群以外，不存在其它真正规子群，则称 G 是**单群**。当然，单群允许有真子群。最简单的单群是素数阶群，它必是循环群，而且据拉格朗日定理知，它不含任何真子群，所以素数阶

群必是交换单群。有趣的是，任一交换单群 G 必是素数阶群。现在我们就来证明这件事。首先指出，因为 G 是交换群，任一子群必是正规子群，所以由 G 是单群知，它不允许存在任何真子群，也即不存在异于 $\{e\}$ 和 G 的子群。任意取定某个 $a\in G$，$a\neq e$，则 $\langle a\rangle$ 是 G 的子群，且 $\langle a\rangle\neq\{e\}$，所以 $G=\langle a\rangle$。如果 G 是无限循环群，则 $\langle a^2\rangle$ 是 $\langle a\rangle$ 的真子群，又与 $\langle a\rangle$ 是单群相矛盾，所以 $G=\langle a\rangle$ 是 n 阶群。如果 n 不是素数，则可分解成 $n=lm$，$1<l$，$m<n$，这样又得到 $\langle a\rangle$ 的真子群 $\langle a^l\rangle$，矛盾。于是证得 G 必是素数阶群。综上所述，我们可得到一个简洁的结论：交换单群就是素数阶群，且必是循环群。既然是交换群的单群已经弄清楚，那末自然要转向考虑不是交换群的单群了！设 G 是某个不是交换群的单群，则 $G\rhd 1$ 是 G 的唯一的正规群列，$G/1=G$ 是唯一的因子群。由 G 不是交换群知，G 不是可解群，所以非交换单群一定不是可解群。换句话说，是可解群的单群一定是交换单群，因而必是素数阶循环群。可以直接证明，当 $n\geqslant 5$ 时，A_n 是非交换单群，据此也可推知，当 $n\geqslant 5$ 时，A_n 不是可解群。

利用单群的概念可以讨论一个有限群何时是可解群。这对于建立一个代数方程能否用根号求解的判别准则是必不可少的。首先可以证明，对有限群来说，必存在一种特殊的正规群列，其每个因子群都是单群。每个因子群都是单群的正规群列称为**合成群列**。例如，S_4 有合成群列

$$S_4\rhd A_4\rhd K_4\rhd H\rhd 1,$$

其中

$$K_4=\{(1),\ (12)(34),\ (13)(24),\ (14)(23)\}$$

$$H=\{(1),\ (12)(34)\}.$$

因为它的因子群的阶依次为2，3，2 和 2，它们都是单群。设 G

是任一有限群。如果 G 是单群，则 $G \rhd 1$ 就是合成群列。否则，必存在真正规子群。因为 G 是有限群，只能有有限个真正规子群，在其中必可选定某个 G_1，使它所含的元素个数最多。这种 G_1 称为 G 的**极大正规子群**。如果这种群不止一个，则可任意取定一个。于是 G/G_1 必是单群(因为 G/G_1 的正规子群必为 K/G_1，其中 $G \rhd K \rhd G_1$)。这样就得到正规群列 $G \rhd G_1 \rhd 1$，它的第一个因子群是单群。对 $G_1 \rhd 1$ 重复上述讨论，可得 $G \rhd G_1 \rhd G_2 \rhd 1$，其中 G_2 是 G_1 的某个极大正规子群，G_1/G_2 是单群。……如此下去，因为 G 是有限群，经有限步后必得某个正规群列

$$G=G_0 \rhd G_1 \rhd G_2 \rhd \cdots \rhd G_{r-1} \rhd G_r=1,$$

每个 G_{i+1} 是 G_i 的极大正规子群，G_i/G_{i+1} 是单群。因此，任一有限群必有合成群列。

定理 8·4 有限群 G 是可解群 $\Longleftrightarrow$ 存在 G 的某个合成群列，其每个因子群都是素数阶群。

证 必要性。因为 G 是有限群，所以可取 G 的某个合成群列

$$G=G_0 \rhd G_1 \rhd G_2 \rhd \cdots \rhd G_{r-1} \rhd G_r=1,$$

既然 G 是可解群，那末每个子群 G_i 都是可解群，因而每个商群 G_i/G_{i+1} 也都是可解群，再据它们都是单群知，它们一定是交换单群，因而必是素数阶群。

充分性。既然在 G 的这个合成群列中，每个因子群都是素数阶群，当然是交换群，而合成群列必是正规群列，所以 G 是可解群。∎

第三章　伽罗瓦扩域与伽罗瓦群

在本章的前两节中，我们将简要地介绍一些关于多项式和线性空间的基本知识。从§3开始则是伽罗瓦理论的核心内容。

§1　域上的多项式

设 F 是某个数集。如果 F 中任意两数相加、相减、相乘和相除(除数$\neq 0$)所得结果仍在 F 中，即 F 关于数的加减乘除(除数$\neq 0$)是封闭的，则称 F 是一个**数域**。易见，C，R 和 Q 都是数域，分别称为复数域，实数域和有理数域。由于两个非零整数相除未必得到整数，所以 Z 不是数域。在§3中将说明，除了这三个数域以外，还存在无限多个其他数域。因为在本书中我们只讨论由数组成的域，所以凡说到域指的都是数域。由域的定义可见，若 F 是一个域，则 F 中元素全体关于数的加法成群 $(F,+)$，F 中非零元素全体关于数的乘法成群 $(F^*,\cdot)$。

取定某个数域 F。所谓 F 上的(一元)**多项式**指的是

$$f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots\cdots+a_ix^i+\cdots\cdots+a_1x+a_0,$$

这里 x 是 F 上未定元(俗称变元)，所有系数 a_i 都是 F 中的

数，首项系数 $a_n\neq 0$。n 是非负整数，称为 $f(x)$ 的次数，记为 $\deg f(x)=n$。特别地，零次多项式就是 F 中的非零常数 $f(x)=a_0\neq 0$。系数全是零的多项式称为零多项式，记为 $f(x)=0$，这与通常所说的方程式 $f(x)=0$ 是两回事。我们不定义零多项式的次数。任给 F 上的两个多项式

$$f(x)=\sum_{i=0}^{n}a_ix^i,\quad g(x)=\sum_{j=0}^{m}b_jx^j,$$

其中 $a_n\neq 0$，$b_m\neq 0$。不妨设 $n\geqslant m$，此时令 $b_n=b_{n-1}=\cdots\cdots=b_{m+1}=0$。规定多项式的加法、减法和乘法如下：

$$f(x)\pm g(x)=\sum_{i=0}^{n}(a_i\pm b_i)x^i.$$

$$f(x)g(x)=\sum_{k=0}^{n+m}c_kx^k,$$

其中系数

$$c_k=a_kb_0+a_{k-1}b_1+\cdots\cdots+a_1b_{k-1}+a_0b_k=\sum_{i+j=k}a_ib_j,$$

$$k=0,\ 1,\ 2,\ \cdots\cdots,\ n+m$$

把域 F 上的一元多项式全体记作

$$F[x]=\left\{f(x)=\sum_{i=0}^{n}a_ix^i\,|\,a_i\in F,\ n\text{ 是非负整数}\right\}。$$

不难一一验证 $F[x]$ 中的元素关于上述运算具有如下基本性质：

(1)交换律

$$f(x)+g(x)=g(x)+f(x),$$
$$f(x)\,g(x)=g(x)\,f(x)。$$

(2)结合律

$$(f(x)+g(x))+h(x)=f(x)+(g(x)+h(x)),$$

$$(f(x)g(x))h(x)=f(x)(g(x)h(x)).$$

(3)分配律

$$f(x)(g(x)+h(x))=f(x)g(x)+f(x)h(x).$$

(4)消去律　如果 $f(x)g(x)=f(x)h(x)$ 且 $f(x)\neq 0$，则 $g(x)=h(x)$。

显然，集合 $F[x]$ 关于多项式的加法、减法和乘法是封闭的。但是，两个多项式相除就未必得到多项式了，这就牵涉到通常所说的**带余除法**。设 F 是取定的域。对 $f(x), g(x)\in F[x]$，其中 $g(x)\neq 0$，必存在唯一的一对 $h(x), r(x)\in F[x]$，使得

$$f(x)=h(x)g(x)+r(x),$$

这里 $r(x)$ 或者是零多项式，或者 $\deg r(x)<\deg g(x)$。$h(x)$ 和 $r(x)$ 分别称为 $f(x)$ 除以 $g(x)$ 的**商式**和**余式**。一种特殊情况是余式 $r(x)=0$，即 $f(x)=h(x)g(x)$，此时就说在 $F[x]$ 中 $g(x)$ **整除** $f(x)$，记为 $g(x)|f(x)$，并称 $g(x)$ 是 $f(x)$ 的**因式**。如果对 $p(x)\in F[x]$，$n=\deg p(x)\geqslant 1$，不存在次数小于 n 的 $f(x)$，$g(x)\in F[x]$ 使 $p(x)=f(x)g(x)$，则称 $p(x)$ 是 $F[x]$ 中的**不可约多项式**，否则，称 $p(x)$ 是 $F[x]$ 中的**可约多项式**。必须指出，一个多项式是否可约，必须针对某个域而言。例如，x^2+1 在 $R[x]$ 中不可约，但在 $C[x]$ 中却可分解为 $x^2+1=(x-\sqrt{-1})(x+\sqrt{-1})$，因而是 $C[x]$ 中的可约多项式。

设 $f(x)$ 和 $g(x)$ 是 $F[x]$ 中两个不同时为零的多项式。如果 $F[x]$ 中的某个多项式 $d(x)$ 满足以下两个条件：

(1) $d(x)|f(x)$, $d(x)|g(x)$, 即 $d(x)$ 是 $f(x)$ 和 $g(x)$ 的公因式。

(2)对任一满足 $d'(x)|f(x)$ 和 $d'(x)|g(x)$ 的 $d'(x)$, 必有 $d'(x)|d(x)$,则称 $d(x)$ 是 $f(x)$ 和 $g(x)$ 的最高公因式。特别地,把 $f(x)$ 和 $g(x)$ 的首项系数为 1 的最高公因式记为 $(f(x),g(x))$。如果 $(f(x),g(x))=1$,则称 $f(x)$ 和 $g(x)$ 是互素的。此时,它们的公因式只能是 F 中的常数。

关于多项式的最高公因式有如下常用的定理。

定理 1·1 (辗转相除法)对于 $F[x]$ 中任意两个不同时为零的多项式 $f(x)$ 和 $g(x)$,必存在 $u(x)$, $v(x)\in F[x]$ 使

$$(f(x),g(x))=u(x)f(x)+v(x)g(x). \tag{1}$$

特别地,若 $f(x)$ 和 $g(x)$ 互素,则有

$$u(x)f(x)+v(x)g(x)=1 \tag{2}$$

证 我们先证明以下事实。若 $f(x)=h(x)g(x)+r(x)$,则

$$(f(x),g(x))=(g(x),r(x)) \tag{3}$$

事实上,记 $d_1(x)=(f(x),g(x))$, $d_2(x)=(g(x),r(x))$。因为

$$r(x)=f(x)-h(x)g(x),$$

所以由 $d_1(x)|f(x)$ 和 $d_1(x)|g(x)$ 得 $d_1(x)|r(x)$, 于是由 $d_2(x)$ 的定义知 $d_1(x)|d_2(x)$。同理, 由 $f(x)=h(x)g(x)+r(x)$ 和 $d_2(x)|g(x)$, $d_2(x)|r(x)$,得 $d_2(x)|f(x)$,又有 $d_2(x)|d_1(x)$. 因为 $d_1(x)$ 和 $d_2(x)$ 的首项系数都是 1, 所以必有 $d_1(x)=d_2(x)$,这就是(3)式。

现在再来证明 (1) 式。如 $g(x)=0$,则由假设知, $f(x)$ 的首项系数 $a_n\neq 0$, 显然有 $(f(x),0)=a_n^{-1}f(x)+1\cdot 0$,这是 (1)

式的特殊情形。设 $g(x)\neq 0$，则可设 $f(x)=h_1(x)g(x)+r_1(x)$，$r_1(x)=0$ 或 $\deg r_1(x)<\deg g(x)$。如果 $r_1(x)=0$，则

$$
\begin{aligned}
(f(x),g(x))&=(h_1(x)g(x),g(x))\\
&=b_m^{-1}g(x)+0\cdot f(x),
\end{aligned}
$$

这里 b_m 是 $g(x)$ 的首项系数，这也是 (1) 式的特殊情形。因此可讨论 $g(x)$ 和 $r_1(x)$ 都不是零多项式的情形。反复利用带余除法可得以下一系列等式

$$
\begin{aligned}
&f(x)=h_1(x)g(x)+r_1(x),\\
&g(x)=h_2(x)r_1(x)+r_2(x),\\
&r_1(x)=h_3(x)r_2(x)+r_3(x),\\
&\cdots\cdots\cdots\cdots\cdots\cdots \qquad\qquad (4)\\
&r_{s-3}(x)=h_{s-1}(x)r_{s-2}(x)+r_{s-1}(x),\\
&r_{s-2}(x)=h_s(x)r_{s-1}(x)+r_s(x),\\
&r_{s-1}(x)=h_{s+1}(x)r_s(x)+r_{s+1}(x),
\end{aligned}
$$

这里 $\deg g(x)>\deg r_1(x)>\deg r_2(x)>\cdots\cdots>\deg r_s(x)>\deg r_{s+1}(x)\geqslant 0$。这就是通常所说的辗转相除法的含义。因为 $\deg g(x)$ 是非负有限数，所以必存在自然数 s 使 $r_s(x)\neq 0$ 而 $r_{s+1}(x)=0$。(因为 F 中任一非零常数必整除任一多项式)。于是根据 (3) 式可得

$$
\begin{aligned}
&(f(x),g(x))=(g(x),r_1(x))=(r_1(x),r_2(x))=\cdots\cdots\\
&=(r_{s-1}(x),r_s(x))=(r_s(x),0)=c^{-1}r_s(x),
\end{aligned}
$$

这里 c 是 $r_s(x)$ 的首项系数．在等式组 (4) 的倒数第二个等式中可解出

$$
r_s(x)=r_{s-2}(x)-h_s(x)r_{s-1}(x),
$$

但 $r_{s-1}(x)$ 和 $r_{s-2}(x)$ 又可根据前面两个等式用其它足标更小的 $h_i(x)$ 和 $r_i(x)$ 表出，所以最后可把 $r_s(x)$ 表为 $f(x)$ 和 $g(x)$ 的线性组合，再除以 $r_s(x)$ 的首项系数 c 即得 (1) 式。据多项式互素的定义，由 (1) 式立得 (2) 式。▌

关于多项式的整除性有以下常用性质：

(1) 若 $f(x)|g(x)$，$g(x)|f(x)$，则存在 $c\in F^*$ 使 $f(x)=c\cdot g(x)$。

(2) 若 $f(x)|g(x)$，$g(x)|h(x)$，则 $f(x)|h(x)$。

(3) 若 $f(x)|g_i(x)$，$i=1,2,\cdots\cdots,n$，则对任意 $u_i(x)\in F[x]$，$i=1,2,\cdots\cdots,n$，必有 $f(x)\Big|\sum_{i=1}^{n}u_i(x)g_i(x)$。

(4) 若 $f(x)|g(x)h(x)$，且 $(f(x),g(x))=1$，则 $f(x)|h(x)$。事实上，可设 $u(x)f(x)+v(x)g(x)=1$，有

$$u(x)f(x)h(x)+v(x)g(x)h(x)=h(x),$$

于是，由 $f(x)|g(x)h(x)$ 立得 $f(x)|h(x)$。

(5) 若 $f_1(x)|g(x)$，$f_2(x)|g(x)$，且 $(f_1(x),f_2(x))=1$，则

$$f_1(x)f_2(x)|g(x)。$$

事实上，可设 $g(x)=f_1(x)h(x)$，则 $f_2(x)|f_1(x)h(x)$。由 $(f_1(x),f_2(x))=1$ 得 $f_2(x)|h(x)$，$f_1(x)f_2(x)|g(x)$。

(6) 若 $p(x)$ 是 $F[x]$ 中不可约多项式，则对任何 $f(x)\in F[x]$，或者 $p(x)|f(x)$，或者 $(p(x),f(x))=1$。由此可知当 $p(x)|f(x)g(x)$ 时必有 $p(x)|f(x)$ 或者 $p(x)|g(x)$。

众所周知，任一自然数 $n\geqslant 2$ 必可唯一地分解为若干个素数的乘积

$$n=p_1^{e_1}p_2^{e_2}\cdots\cdots p_s^{e_s},$$

这里 $p_1, p_2, \cdots p_s$ 是 s 个两两互异的素数，$e_1, e_2, \cdots, e_s$ 是自然数。对于域 F 上的多项式也有类似的结果. 任一次数 $\geqslant 1$ 的 $f(x) \in F[x]$ 必可唯一地分解成

$$f(x) = ap_1^{e_1}(x)p_2^{e_2}(x)\cdots\cdots p_s^{e_s}(x),$$

这里 $p_i(x)$ 都是 $F[x]$ 中的两两互异的首项系数是 1 的不可约多项式，e_i 是自然数，a 是 $f(x)$ 的首项系数。$p_i(x)$ 称为 $f(x)$ 的 e_i 重因式。给定域 F 上多项式

$$f(x) = a_n x^n + \cdots\cdots + a_i x^i + \cdots\cdots + a_1 x + a_0,$$

某个复数 α 称为 $f(x)$ 的一个根，如果

$$f(\alpha) = a_n \alpha^n + \cdots\cdots + a_i \alpha^i + \cdots\cdots + a_1 \alpha + a_0 = 0.$$

当然，这个 α 未必属于 F，但据代数学基本定理知，这种复数 α 一定存在。若$\deg f(x) = n$，则在 $C[x]$ 中有分解式

$$f(x) = a_n(x-\alpha_1)^{e_1}(x-\alpha_2)^{e_2}\cdots\cdots(x-\alpha_s)^{e_s},$$

这里 $\alpha_1, \alpha_2, \cdots, \alpha_s$ 是 $f(x)$ 的不同的根，$e_1, e_2, \cdots\cdots, e_s$ 是自然数。此时，称 α_i 是 $f(x)$ 的 e_i 重根，$i = 1, 2, \cdots\cdots, s$. 对于给定的 $f(x)$，我们希望不通过求根就可以判定它有没有重根。为此，需引进多项式导数的概念。对于给定的 n 次多项式

$$f(x) = a_n x^n + \cdots\cdots + a_k x^k + \cdots + a_1 x + a_0 = \sum_{k=0}^{n} a_k x^k.$$

定义它的一阶导数是

$$f'(x) = na_n x^{n-1} + \cdots + ka_k x^{k-1} + \cdots + a_1 = \sum_{k=1}^{n} ka_k x^{k-1},$$

它是 $n-1$ 次多项式。我们可直接验证有如下求导公式：

$$(f(x)+g(x))'=f'(x)+g'(x),$$
$$(f(x)g(x))'=f'(x)g(x)+f(x)g'(x).$$

现在可以证明

定理 1·2　$f(x)$没有重根$\Longleftrightarrow(f(x),f'(x))=1$。

证　必要性。设 $f(x)$没有重根，不妨设 $f(x)$ 的首项系数是 1。则在 $C[x]$ 中有

$$f(x)=(x-\alpha_1)\cdots\cdots(x-\alpha_i)\cdots\cdots(x-\alpha_n)=\prod_{i=1}^{n}(x-\alpha_i),$$

这里 $\alpha_1, \alpha_2, \cdots\cdots, \alpha_n$ 是 $f(x)$ 的两两互异的根。于是根据求导公式得

$$f'(x)=\prod_{i=2}^{n}(x-\alpha_i)+\cdots+\prod_{\substack{i=1\\ i\neq j}}^{n}(x-\alpha_i)+\cdots+\prod_{i=1}^{n-1}(x-\alpha_i).$$

任意取定 $f(x)$ 的某个根 α_j，有

$$f'(\alpha_j)=0+\cdots\cdots+\prod_{\substack{i=1\\ i\neq j}}^{n}(\alpha_j-\alpha_i)+\cdots\cdots+0\neq 0,$$

这说明 $f(x)$ 与 $f'(x)$ 无公共根，所以$(f(x),f'(x))=1$。

充分性。采用反证法。如果α是$f(x)$的某个e重根，$e\geqslant 2$，则在 $C[x]$ 中 $f(x)$ 必可分解为

$$f(x)=(x-\alpha)^e g(x),$$

于是

$$f'(x)=e(x-\alpha)^{e-1}g(x)+(x-\alpha)^e g'(x)$$
$$=(x-\alpha)^{e-1}[eg(x)+(x-\alpha)g'(x)].$$

由 $e-1\geqslant 1$ 知必有 $f'(\alpha)=0$，所以 α 是 $f(x)$ 和 $f'(x)$ 的公根。如果$(f(x),f'(x))=1$，则可设 $u(x)f(x)+v(x)f'(x)=1$，将 $x=\alpha$ 代入即得 $0=1$ 之矛盾，所以 $(f(x),f'(x))\neq 1$。▌

推论 任一域 F 上的任一不可约多项式一定没有重根。

证 设 $p(x)$ 是 $F[x]$ 中的不可约多项式,则对 $p'(x)\in F[x]$,或者 $p(x)\mid p'(x)$ 或者 $(p(x),p'(x))=1$。但是,$\deg p(x)>\deg p'(x)$ 且 $p'(x)\neq 0$,$p(x)$ 不可能是 $p'(x)$ 的因式,所以必有 $(p(x),p'(x))=1$,$p(x)$ 没有重根。▌

由于 $F[x]$ 关于多项式的除法不封闭,所以我们要引出上述的整除性理论。进一步还可模仿用整数集造出有理数集的方法,考虑集合:

$$F(x)=\left\{\frac{f(x)}{g(x)}\,\middle|\,\begin{array}{c}f(x),g(x)\in F[x]\\ g(x)\neq 0\end{array}\right\},$$

易见它关于以下运算都是封闭的:

$$\frac{f_1(x)}{g_1(x)}\pm\frac{f_2(x)}{g_2(x)}=\frac{f_1(x)g_2(x)\pm g_1(x)f_2(x)}{g_1(x)g_2(x)},$$

$$\frac{f_1(x)}{g_1(x)}\cdot\frac{f_2(x)}{g_2(x)}=\frac{f_1(x)f_2(x)}{g_1(x)g_2(x)},$$

$$\frac{f_1(x)}{g_1(x)}\Big/\frac{f_2(x)}{g_2(x)}=\frac{f_1(x)g_2(x)}{g_1(x)f_2(x)}$$

通常把 $F(x)$ 称为一元有理分式域,这里的“有理”两字指的是分子分母都是多项式。

以上讨论的都是仅含一个变元 x 的情形。在伽罗瓦理论中还要用到含多个变元的多项式和有理分式。例如:

$$f(x_1,x_2,x_3)=2x_1^3x_2x_3^2+3x_1^2x_2^3x_3-5x_1x_2^4x_3$$

就是一个三元多项式。以下 4 个四元多项式

$$\sigma_1=x_1+x_2+x_3+x_4,$$

$$\sigma_2=x_1x_2+x_1x_3+x_1x_4+x_2x_3+x_2x_4+x_3x_4$$
$$\sigma_3=x_1x_2x_3+x_1x_2x_4+x_1x_3x_4+x_2x_3x_4$$
$$\sigma_4=x_1x_2x_3x_4$$

有一个共同的特点，就是把 4 个变元的 4 个下标 1,2,3,4 作任何一个 4 阶置换，所得到的仍然是原来的四元多项式，这说明它们具有上述意义下的“对称性”。通常把这 4 个多项式称为初等对称多项式。一般地，含 n 个变元的 n 个**初等对称多项式**为

$$\sigma_1=\sum_i x_i=x_1+x_2+\cdots\cdots+x_n,$$

$$\sigma_2=\sum_{1\leq i_1<i_2\leq n}x_{i_1}x_{i_2}=x_1x_2+x_1x_3+\cdots+x_1x_n+x_2x_3+\cdots+x_{n-1}x_n,$$

$$\cdots\cdots\cdots\cdots$$

$$\sigma_k=\sum_{1\leq i_1<i_2<\cdots<i_k\leq n}x_{i_1}x_{i_2}\cdots x_{i_k},$$

$$\cdots\cdots\cdots\cdots$$

$$\sigma_n=x_1x_2\cdots\cdots x_n,$$

这里 σ_k 是所有可能的 k 个 x_i 的乘积之和，不过这 k 个 x_i 的下标必须满足 $1\leqslant i_1<i_2<\cdots\cdots<i_k\leqslant n$。易见，它们在任一 n 阶置换下都不变。利用初等对称多项式可得到著名的韦达(F.Vieta,1540～1603)公式．用它可刻划一元多项式的系数与根之间的关系，即

定理 1·3　如果 $x_1,x_2,\cdots\cdots,x_n$ 是 n 次多项式

$$f(x)=x^n+a_1x^{n-1}+\cdots\cdots+a_kx^{n-k}+\cdots\cdots+a_{n-1}x+a_n$$

的 n 个根，(注意系数足标与 x 的方幂之间的关系）则必有如下关系式

$$\sigma_1=-a_1,\ \sigma_2=a_2,\cdots,\ \sigma_k=(-1)^k a_k,\cdots\cdots,$$
$$\sigma_n=(-1)^n a_n,$$

这里 $\sigma_1,\sigma_2,\cdots,\sigma_n$ 就是 $x_1,x_2,\cdots,x_n$ 的 n 个初等对称多项式.

事实上，比较等式

$$x^n+a_1x^{n-1}+\cdots\cdots+a_kx^{n-k}+\cdots\cdots+a_{n-1}x+a_n$$
$$=(x-x_1)(x-x_2)\cdots\cdots(x-x_n)$$

两边 x 的同次项的系数就可得到所需要的关系式.

域 F 上的 n 元多项式的一般形式可写为

$$f(x_1,x_2,\cdots,x_n)=\sum a_{k_1k_2\cdots k_n}x_1^{k_1}x_2^{k_2}\cdots\cdots x_n^{k_n},$$

这里，所有系数 $a_{k_1k_2\cdots k_n}$ 都是 F 中数. 称这种多项式是**对称多项式**，如果它在任一 $\tau\in S_n$ 之下不变，确切地说，若把 i 在 n 阶置换 τ 之下的象记为 j_i，则有

$$f(x_1,\cdots,x_i,\cdots,x_n)=f(x_{j_1},\cdots,x_{j_i},\cdots,x_{j_n}),$$

即把 x_i 换成 x_{j_i}，多项式不变，$i=1,2,\cdots,n$。关于对称多项式有以下重要定理：

定理 1·4 (对称多项式基本定理)对于 F 上的任一 n 元对称多项式 $f(x_1,x_2,\cdots\cdots,x_n)$，必存在 F 上唯一的 n 元多项式 $\varphi(y_1,y_2,\cdots,y_n)$ 使

$$f(x_1,x_2,\cdots,x_n)=\varphi(\sigma_1,\sigma_2,\cdots,\sigma_n),$$

这里 $\sigma_1,\sigma_2,\cdots,\sigma_n$ 是 $x_1,x_2,\cdots,x_n$ 的 n 个初等对称多项式. 这就是说，任一 n 元对称多项式都可唯一地表为 n 个 n 元初

等对称多项式的多项式。

例如，设 $f(x)=x^2+bx+c$ 的根为 x_1, x_2, 则它的判别式

$$D=(x_1-x_2)^2=(x_1+x_2)^2-4x_1x_2=\sigma_1^2-4\sigma_2。$$

用 $\sigma_1=-b$, $\sigma_2=c$ 代入就得到通常所见的二次多项式的判别式：

$$D=b^2-4c。$$

又如，设 $f(x)=x^3+a_1x^2+a_2x+a_3$ 的三个根为 x_1, x_2 和 x_3, 则它的判别式

$$D=(x_1-x_2)^2(x_1-x_3)^2(x_2-x_3)^2$$

显然是对称多项式。可以验证 D 可表为 x_1, x_2, x_3 的三个初等对称多项式 σ_1, σ_2 和 σ_3 的多项式：

$$D=-4\sigma_1^3\sigma_3+\sigma_1^2\sigma_2^2+18\sigma_1\sigma_2\sigma_3-4\sigma_2^3-27\sigma_3^2,$$

再换成 $f(x)$ 的系数，可得

$$D=-4a_1^3a_3+a_1^2a_2^2+18a_1a_2a_3-4a_2^3-27a_3^2,$$

一个三次方程有重根当且仅当上述判别式 $D=0$。

通常，我们把F上 n 元多项式全体记为 $F[x_1,x_2,\cdots\cdots,x_n]$，而

$$F(x_1,x_2,\cdots\cdots,x_n)=\left\{\frac{f(x_1,x_2,\cdots,x_n)}{g(x_1,x_2,\cdots,x_n)}\;\middle|\;\begin{matrix}f,g\in F[x_1,x_2,\cdots,x_n]\\ g\neq 0\end{matrix}\right\}$$

称为 n 元有理分式域，它的元素都是 n 元多项式的商。

§2 域上的线性空间

在平面上取定直角坐标系{XOY}，则平面上任一点 P 都可用 2 维实向量 (x,y) 表示，x 是 P 的横坐标，y 是 P 的纵坐标，它们都是实数。易见 2 维实向量全体

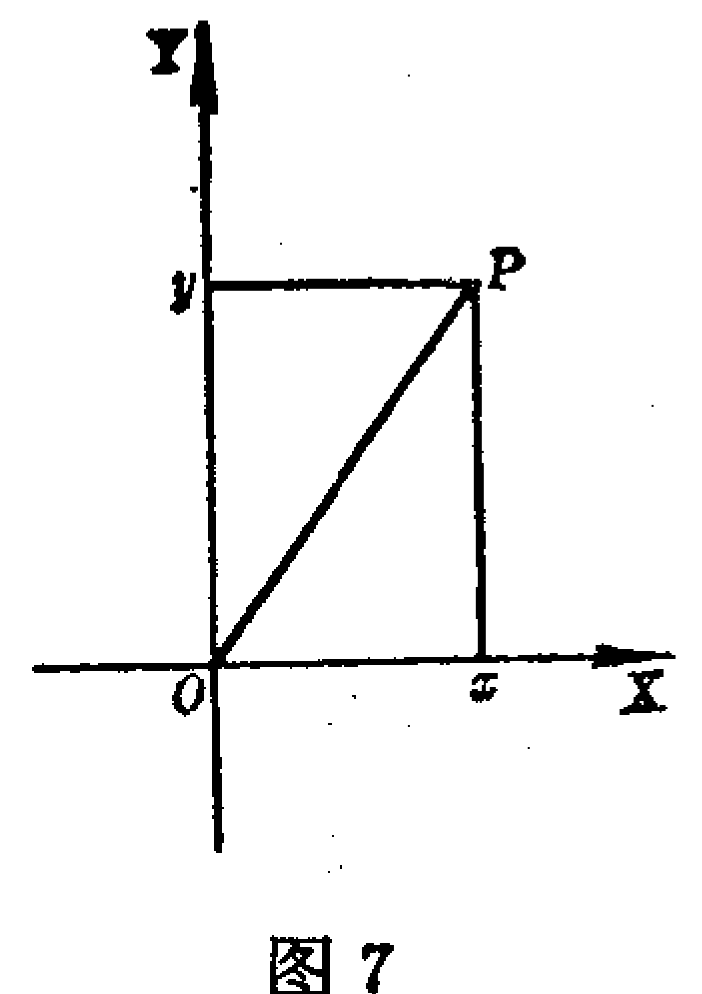


图 7

$$V=\{(x,y)\,|\,x,y\in R\}$$

关于向量加法

$$(x_1,y_1)+(x_2,y_2)=(x_1+x_2,\ y_1+y_2)$$

成交换群。另外在 V 中还可定义一种数与向量的乘法：

$$a(x,y)=(ax,ay),\ \ \forall a\in R,\ (x,y)\in V。$$

运算结果仍是 V 中向量，而且还满足如下等式：

$$1\cdot(x,y)=(x,y),\quad (ab)(x,y)=a(b(x,y)),$$

$$(a+b)(x,y)=a(x,y)+b(x,y),$$

$$a[(x_1,y_1)+(x_2,y_2)]=a(x_1,y_1)+a(x_2,y_2)。$$

我们就说 V 是 R 上的 2 维线性空间(又称向量空间)。域上的线性空间的一般定义如下：

定义 2·1　设 F 是域，V 是非空集合，在 V 中定义了加法 $\alpha+\beta$，$\alpha,\beta\in V$。且对 $a\in F$，$\alpha\in V$，又定义了数量乘法 $a\alpha$，运算结果都是 V 中确定的元素。如果满足以下条件：

（Ⅰ）V 关于加法成交换群，

（Ⅱ）数乘结合律：$(ab)\alpha=a(b\alpha)$，$\forall a,b\in F$，$\alpha\in V$，

（Ⅲ）数乘分配律：对$a,b\in F$，$\alpha,\beta\in V$有

$$(a+b)\alpha=a\alpha+b\alpha, \qquad a(\alpha+\beta)=a\alpha+a\beta,$$

（Ⅳ）$1\cdot\alpha=\alpha$，$\forall\alpha\in V$，

则称 V 是 F 上的一个**线性空间**，可简记为F-V。

不难验证，域 F 上一元多项式全体

$$F[x]=\left\{\sum_{i=0}^{n}a_i x^i \middle| a_i\in F,\ n\text{是非负整数}\right\}$$

是 F 上的线性空间，其中加法就是多项式加法，数乘就是数与多项式的乘法：$b\left(\sum_{i=0}^{n}a_i x^i\right)=\sum_{i=0}^{n}ba_i x^i$。类似地，$R$ 上的 n 阶方阵全体 $M_n(R)$ 关于矩阵的加法和数与矩阵的乘法也成 R 上的线性空间。由于两个可逆阵之和未必是可逆阵，所以 $GL_n(R)$ 关于这两种运算不成线性空间。

线性空间的维数是它的一个很重要的特征。设 V 是域 F 上的线性空间，$\alpha_1,\alpha_2,\cdots\cdots,\alpha_r$ 是 V 中一组元素。如果对某个 $\alpha\in V$，存在 $a_1,a_2,\cdots,a_r\in F$ 使得

$$\alpha=a_1\alpha_1+a_2\alpha_2+\cdots\cdots+a_r\alpha_r,$$

则称 α 可经 $\alpha_1,\alpha_2,\cdots,\alpha_r$ **线性表出**，其中 $a_1,a_2,\cdots\cdots,a_r$ 称为**表出系数**。我们把加法群 $(V,+)$ 中的单位元记作 θ，读作零元，它与数字零不同。易见，θ 必可经 V 中任一元素组线性表出，表出系数全是 0。V 中元素组 $\alpha_1,\alpha_2,\cdots\cdots,\alpha_r$ 称为**线性相关**，如果存在不全为 0 的 $k_1,k_2,\cdots\cdots,k_r\in F$ 使

$$k_1\alpha_1+k_2\alpha_2+\cdots\cdots+k_r\alpha_r=\theta$$

既然必存在某个 k_i 不是 0，不妨设 $k_\gamma \neq 0$，则 α_γ 必可经 α_1，α_2，……，$\alpha_{\gamma-1}$ 线性表出

$$\alpha_\gamma = -\frac{1}{k_\gamma}(k_1\alpha_1 + k_2\alpha_2 + \cdots\cdots + k_{\gamma-1}\alpha_{\gamma-1}).$$

不是线性相关的元素组称为**线性无关**元素组，即

$$k_1\alpha_1 + k_2\alpha_2 + \cdots\cdots + k_\gamma\alpha_\gamma = \theta$$

当且仅当所有 k_i 都是 0 时成立。由上述定义可见，V 中元素组是否线性相关，与 V 的系数域 F 密切相关，所以有必要时需明确地把它们称为 F- 线性相关或 F- 线性无关。

定义 2·2　设 V 是域 F 上的线性空间。如果 V 中存在 n 个线性无关的元素，但不存在更多个数的线性无关的元素，则称 V 是 F 上的 **n 维线性空间**，统称为有限维线性空间。存在无限多个线性无关元素的线性空间称为无限维线性空间。

由定义可见，有限维线性空间的维数是唯一确定的。若 V 是 F 上 n 维线性空间，则 V 中任何一组个数大于 n 的元素组必定是线性相关的。这一个事实以后经常要用到。若 V 是 F 上 n 维线性空间，这仅说明存在 n 个线性无关的元素，但这种元素组未必只有一个。n 维线性空间中任意一个含 n 个元素的线性无关组都称为 V 中的一个 F- **基**。设 $\alpha_1, \alpha_2, \cdots\cdots, \alpha_n$ 是 V 中的一个 F- 基，则它有两个特征性质。第一，任取 $\alpha \in V$，因为 V 的维数是 n，所以 $n+1$ 个元素 $\alpha_1, \cdots\cdots, \alpha_n, \alpha$ 必定线性相关，即必存在不全为 0 的 $a_1, \cdots\cdots, a_n, a \in F$ 使

$$a_1\alpha_1 + \cdots\cdots + a_n\alpha_n + a\alpha = \theta.$$

如果 $a=0$，则 $a_1, \cdots\cdots, a_n$ 不全为 0，这与 $\alpha_1, \cdots\cdots, \alpha_n$ 是线性

无关的假设矛盾，所以 $a\neq 0$，于是必有

$$\alpha=-\frac{1}{a}(a_1\alpha_1+\cdots\cdots+a_n\alpha_n),$$

这就是说任一 $\alpha\in V$ 都可经基中元素线性表出。第二，这种表示法是唯一的。事实上，设

$$\alpha=\sum_{i=1}^{n}a_i\alpha_i=\sum_{i=1}^{n}b_i\alpha_i,\quad a_i,b_i\in F,$$

则

$$\sum_{i=1}^{n}(a_i-b_i)\alpha_i=\theta,$$

但 $\alpha_1,\cdots\cdots,\alpha_n$ 是线性无关的，必有 $a_i-b_i=0$，$a_i=b_i$，$i=1,2,\cdots\cdots,n$。反之，V 中具有这两个特征性质的元素组 $\alpha_1,\cdots\cdots,\alpha_n$ 必是 V 中的 F-基。这只要证明 $\alpha_1,\cdots,\alpha_n$ 线性无关就可以了。事实上，如果它们线性相关，即存在不全为 0 的 $a_1,\cdots,a_n$ 使得

$$a_1\alpha_1+a_2\alpha_2+\cdots+a_n\alpha_n=\theta,$$

但显然又有

$$0\cdot\alpha_1+0\cdot\alpha_2+\cdots\cdots+0\cdot\alpha_n=\theta,$$

所以零元 θ 的表示法就不唯一了，这与条件矛盾。

我们来看一些实例。在 R 上的线性空间

$$V=\{(x,y)\,|\,x,y\in R\}$$

中，取 $\alpha_1=(1,0)$，$\alpha_2=(0,1)$。易见任一 $\alpha=(x,y)$ 必可唯一地表为 $\alpha=x\alpha_1+y\alpha_2$，所以 α_1,α_2 是一个 R-基，V 是 R 上 2

维线性空间。在

$$F[x]=\left\{\sum_{i=0}^{n} a_i x^i \,\middle|\, a_i\in F,\ n\text{是非负整数}\right\}$$

中取如下无限多个多项式

$$\alpha_0=1,\ \alpha_1=x,\ \alpha_2=x^2,\cdots\cdots,\alpha_k=x^k,\cdots\cdots。$$

显然，它们构成 $F[x]$ 中的一个 F- 基，所以 $F[x]$ 是 F 上的无限维线性空间。但是，对于一个确定的自然数 n 来说，次数不超过 n 的多项式全体

$$F[x]_n=\left\{\sum_{i=0}^{n} a_i x^i \,\middle|\, a_i\in F\right\}$$

也是 F 上的线性空间，(请读者自己证一下)，然而它却有如下有限基

$$\alpha_0=1,\ \alpha_1=x,\ \alpha_2=x^2,\cdots\cdots,\alpha_n=x^n。$$

所以 $F[x]_n$ 是 F 上 $n+1$ 维线性空间。又如 $M_n(R)$ 是 R 上 n^2 维线性空间。用 E_{ij} 表示这样的一个 n 阶方阵，它的 (i,j) 位置上的元素是 1，其它位置上的元素全是 0。这种矩阵共有 n^2 个，它们构成 $M_n(R)$ 中的一个 R- 基。

最后，我们介绍一下线性空间的同构概念。

定义 2·3 设 V 和 $\overline{V}$ 是同一个域 F 上的两个线性空间。如果存在 V 到 $\overline{V}$ 的双射 σ，满足

(1) $(\alpha+\beta)^\sigma=\alpha^\sigma+\beta^\sigma,\quad \forall\alpha,\beta\in V,$

(2) $(a\alpha)^\sigma=a\alpha^\sigma,\qquad \forall a\in F,\ \alpha\in V,$

则称 V 和 $\overline{V}$ 是同构的，记为 $V\overset{\sigma}{\cong}\overline{V}$。

定理 2·1 设 $V\cong\overline{V}$，则 $\alpha_1,\alpha_2,\cdots\cdots,\alpha_r$ 是 V 中线性相关元素组 $\Longleftrightarrow \alpha_1^\sigma,\alpha_2^\sigma,\cdots\cdots,\alpha_r^\sigma$ 是 $\overline{V}$ 中线性相关元素组。因而，同构的线性空间必有相同的维数。

证 必要性。设 $\alpha_1,\alpha_2,\cdots\cdots,\alpha_r$ 线性相关，则存在不全为 0 的 $a_1,a_2,\cdots\cdots,a_r$ 使

$$a_1\alpha_1+a_2\alpha_2+\cdots+a_r\alpha_r=\theta。$$

根据同构 σ 的定义，而且注意到 σ 也是加法群 $(V,+)$ 与 $(\overline{V},+)$ 之间的群同构，它把单位元 θ 变为单位元 $\overline{\theta}$，所以

$$a_1\alpha_1^\sigma+a_2\alpha_2^\sigma+\cdots+a_r\alpha_r^\sigma=\overline{\theta},$$

这说明 $\alpha_1^\sigma,\alpha_2^\sigma,\cdots\cdots,\alpha_r^\sigma$ 也是线性相关的。

充分性。设 $\alpha_1^\sigma,\alpha_2^\sigma,\cdots\cdots,\alpha_r^\sigma$ 线性相关，则存在不全为 0 的 $a_1,a_2,\cdots\cdots,a_r$ 使

$$a_1\alpha_1^\sigma+a_2\alpha_2^\sigma+\cdots+a_r\alpha_r^\sigma=\overline{\theta}.$$

仍据 σ 的定义得

$$(a_1\alpha_1+a_2\alpha_2+\cdots\cdots+a_n\alpha_n)^\sigma=\overline{\theta},$$

但 σ 是单射，必有 $\theta^\sigma=\overline{\theta}$，所以，

$$a_1\alpha_1+a_2\alpha_2+\cdots\cdots+a_n\alpha_n=\theta,$$

即 $\alpha_1,\alpha_2\cdots,\alpha_n$ 线性相关。▮

设 V 是 F 上 n 维线性空间，任意取定一个基 $\alpha_1,\alpha_2,\cdots,\alpha_n$，则任一 $\alpha\in V$ 必可唯一地表为

$$\alpha=a_1\alpha_1+a_2\alpha_2+\cdots+a_n\alpha_n.$$

把这 n 个数 $a_i\in F$ 排成长度为 n 的有序组 $(a_1,a_2,\cdots,a_n)$，

则它由 α 唯一确定，把它称为 α 在这个基下的**坐标向量**。考虑集合

$$F^n=\{(a_1,a_2,\cdots,a_n)\,|\,a_n\in F\}.$$

易证 F^n 关于以下运算

$$(a_1,\cdots\cdots,a_n)+(b_1,\cdots\cdots,b_n)=(a_1+b_1,\cdots\cdots,a_n+b_n),$$

$$a(a_1,\cdots\cdots,a_n)=(aa_1,\cdots\cdots,aa_n)$$

也成 F 上的 n 维线性空间，而且 V 与 F^n 是同构的，同构映射就是对 V 中元素取坐标向量（在取定某个基的前提下）。根据这个事实可以证明

定理 2·2　域 F 上两个有限维线性空间同构 $\Longleftrightarrow$ 它们的维数相同。

证　必要性就是定理 2·1 所述，现证充分性。设 V_1 和 V_2 都是 F 上的 n 维线性空间，则有

$$V_1\overset{\sigma}{\cong}F^n,\quad V_2\overset{\tau}{\cong}F^n.$$

但 τ 是双射，且易证逆映射 τ^{-1} 是 F^n 到 V_2 的同构，即 $F^n\overset{\tau^{-1}}{\cong}V_2$. 所以 $V_1\overset{\rho}{\cong}V_2$，其中 $\rho=\sigma\tau^{-1}$ 是 V_1 到 V_2 的同构。▌

§3　有限扩域与单代数扩域

在 §1 中已说过，Q, R 和 C 是三个数域。必须指出，除了 Q, R, C 以外，成域的数集还有很多很多。例如实数集 R 的如下真子集

$$Q(\sqrt{2})=\{a+b\sqrt{2}\,|\,a,b\in Q\}$$

也是域(这里$Q(\sqrt{2})$是一个完整的记号)。这是因为

$$(a+b\sqrt{2})\pm(c+d\sqrt{2})=(a\pm c)+(b\pm d)\sqrt{2},$$

$$(a+b\sqrt{2})(c+d\sqrt{2})=(ac+2bd)+(ad+bc)\sqrt{2},$$

$$\frac{a+b\sqrt{2}}{c+d\sqrt{2}}=\frac{1}{c^2-2d^2}\left[\left(ac-2bd\right)+\left(bc-ad\right)\sqrt{2}\right],$$

其中$c+d\sqrt{2}\neq 0$,仍是$Q(\sqrt{2})$中数。同理,

$$Q(\sqrt{3})=\{a+b\sqrt{3}\mid a,b\in Q\}$$

也是域。这些域都比Q大,称为Q的扩域,称Q是它们的子域。一般地,若F和E是两个域,如果$F\subseteq E$,则称E是F的**扩域**,F是E的**子域**。如果$F\subset E$,即F是E的真子集,则称E是F的**真扩域**,F是E的**真子域**。设F是任一域。由于它对减法和除法封闭,F中必包含0、1和-1,再由加法封闭性知,它包含所有整数n,再由除法封闭性知,它包含所有的有理数n/m。这说明任一域都是Q的扩域,有理数域是最小的域。因为一个代数方程求根总是在某个域中进行的,若它在某个域中无根,但可能在某个扩域中有根,所以扩域这个概念是非常重要的。

关于扩域,我们要引进一个很重要的观点。设E是域F的扩域,则域E的加法群$(E,+)$可以看成域F上的线性空间。事实上,$(E,+)$是一个交换群,且对任一$f\in F$,$e\in E$,必有$fe\in E$且满足$(f_1f_2)e=f_1(f_2e)$,$(f_1+f_2)e=f_1e+f_2e$,$f(e_1+e_2)=fe_1+fe_2$,$1\cdot e=e$,这里$f_1,f_2,f\in F$,$e_1,e_2,e\in E$。(由于ef未必属于F,所以$(F,+)$不能看成E上的线性空间)。如果这个线性空间是n维的,则可任意取定一个基α_1,

$\alpha_2,\cdots\cdots,\alpha_n$，它们都是 E 中的数，而且任一 $a\in E$ 必可唯一地表为

$$a=a_1\alpha_1+a_2\alpha_2+\cdots\cdots+a_n\alpha_n,$$

这里，所有表出系数 a_i 都是 F 中的数。我们把 $\{\alpha_1,\alpha_2,\cdots\cdots,\alpha_n\}$ 称为域 E 中的一个 F- 基，表示这个基与 F 有关。此时，称 E 是 F 的 n 次扩域，记为 $[E:F]=n$。有时，我们并不关心有限数 n 的确切数值，就可径直称 E 是 F 的有限扩域，用 $[E:F]<\infty$ 表示。例如，$[Q(\sqrt{2}):Q]=2$，因为 $\{1,\sqrt{2}\}$ 是它的一个 Q- 基。注意，数集

$$F=\{a+b\sqrt{2}+c\sqrt{3}\mid a,b,c\in Q\}$$

不是域，因为 $\sqrt{2}\cdot\sqrt{3}=\sqrt{6}\notin F$。但是可以验证，数集

$$Q(\sqrt{2},\sqrt{3})=\{a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6}\mid a,b,c,d\in Q\}$$

是 Q 的 4 次扩域，$\{1,\sqrt{2},\sqrt{3},\sqrt{6}\}$ 是一个 Q- 基。

我们考虑以下三个域

$$Q\subset Q(\sqrt{2})\subset Q(\sqrt{2},\sqrt{3}).$$

因为

$$a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6}=(a+b\sqrt{2})+(c+d\sqrt{2})\sqrt{3},$$

所以 $[Q(\sqrt{2},\sqrt{3}):Q(\sqrt{2})]=2$，$\{1,\sqrt{3}\}$ 是 $Q(\sqrt{2},\sqrt{3})$ 中的一个 $Q(\sqrt{2})$-基。于是，我们得到一个等式

$$[Q(\sqrt{2},\sqrt{3}):Q]$$
$$=[Q(\sqrt{2},\sqrt{3}):Q(\sqrt{2})][Q(\sqrt{2}):Q].$$

可以证明，这对任意扩域都是正确的。

定理 3·1　设 $F\subseteq E\subseteq K$ 是三个域。如果 $[K:F]<\infty$，则

$[K:E]<\infty$，$[E:F]<\infty$，且有次数等式

$$[K:F]=[K:E][E:F]。 \tag{1}$$

证 首先，由扩域次数的定义立刻可见，当 $[K:F]<\infty$ 时，必有 $[K:E]<\infty$，$[E:F]<\infty$。设 $[K:E]=m$，$[E:F]=n$。在 K 中任取一个 E-基 $\{\alpha_1,\cdots\cdots,\alpha_m\}$，在 E 中任取一个 F-基 $\{\beta_1,\cdots\cdots,\beta_n\}$。任取 $a\in K$，它必可表为

$$a=\sum_{i=1}^{m}a_i\alpha_i,\quad a_i\in E,$$

但这些 a_i 又都可表为

$$a_i=\sum_{j=1}^{n}b_{ij}\beta_j,\quad b_{ij}\in F,$$

于是

$$a=\sum_{i=1}^{m}\sum_{j=1}^{n}b_{ij}\beta_j\alpha_i,\quad b_{ij}\in F。$$

设另有

$$a=\sum_{i=1}^{m}\sum_{j=1}^{n}c_{ij}\beta_j\alpha_i,\quad c_{ij}\in F,$$

则

$$\sum_{i=1}^{m}\left[\sum_{j=1}^{n}\left(b_{ij}-c_{ij}\right)\beta_j\right]\alpha_i=0。$$

因为 $\{\alpha_1,\cdots,\alpha_m\}$ 是 K 中的 E-基，0 的表示法仅有一种：

$$0=0\cdot\alpha_1+0\cdot\alpha_2+\cdots\cdots+0\cdot\alpha_m,$$

所以必有

$$\sum_{j=1}^{n}(b_{ij}-c_{ij})\beta_j=0,\quad i=1,2,\cdots\cdots,m。$$

再据 $\{\beta_1,\cdots\cdots,\beta_n\}$ 是 E 中的 F- 基,立得

$$b_{ij}=c_{ij},\quad i=1,2,\cdots\cdots,m;\ j=1,2,\cdots\cdots,n。$$

这说明 K 中任意数都可唯一地表示为 mn 个数 $\beta_j\alpha_i(i=1,\cdots,m;\ j=1,\cdots,n)$的线性组合,系数属于 F。所以 $\{\beta_j\alpha_i,j=1,\cdots\cdots,n;\ i=1,\cdots\cdots,m\}$ 是 K 中的 F- 基。(1) 式得证。▌

下面我们要引进域的单代数扩域的概念，它在扩域理论中占着非常重要的地位。设 F 是任一域。考虑 F 上的一元多项式全体

$$F[x]=\{f(x)=a_0+a_1x+\cdots+a_nx^n\mid a_i\in F,\ n\text{是非负整数}\}.$$

易见,它关于多项式的加法、减法和乘法是封闭的。

定义 3·1 称数 α 是域 F 上代数元，如果在 $F[x]$ 中存在某个非零多项式 $f(x)$ 使 $f(\alpha)=0$。否则，称 α 是域 F 上超越元。

由定义可见,任一 $f(x)\in F[x]$ 的根都是 F 上代数元。设 E 是域 F 的扩域。如果 α 是 F 上代数元,则 α 是某个 $f(x)\in F[x]$ 的根,但 $f(x)$ 也是 $E[x]$ 中的多项式,所以 α 也是 E 上代数元。例如 $\sqrt{-1}$ 是 $x^2+1=0$的根，所以 $\sqrt{-1}$ 既是 Q 上代数元,又是 R 上代数元。但是，E 上代数元未必是 F 上代数元。对于 F 中任一数 α,因为它是 $x-\alpha\in F[x]$ 的根,所以 α 必是 F 上代数元。例如,圆周率 π 和自然对数的底 e 都是实数,都是 R 上代数元,但都是 Q 上超越元,因为它们不可能是某个有理系数多项式的根。这些事实告诉我们，代数元和超越元必须针对某个域而言，笼统地说某数是代数元或超

越元是毫无意义的。

设 F 是域，α 是 F 上代数元。当然，在 $F[x]$ 中以 α 为根的多项式有无限多个，其中首项系数为 1 的次数最低者称为 α 在 F 上的最小多项式。易见，它是唯一确定的，而且在 $F[x]$ 中不可约（在 F 的某个扩域中它可能是可约的）。把这个 α 添加到 F 上得到 F 的如下扩域

$$F(\alpha)=\left\{\frac{f(\alpha)}{g(\alpha)}\,\middle|\, f(x),\ g(x)\in F[x],\ \ g(\alpha)\neq 0\right\},$$

它就是把 α 代入 F 上的所有有理分式 $f(x)/g(x)$ 后所得的数全体。注意，$F(\alpha)$ 并不是 F 和单个元素 α 的集合并，而是按上述定义生成的一个域。我们把 $F(\alpha)$ 称为 F 的单代数扩域，~~就是添加单个代数元所得~~的扩域。例如，C 是 R 的单代数扩域

$$C=R(\sqrt{-1})=\{a+b\sqrt{-1}\mid a,b\in R\}.$$

事实上，利用 $(\sqrt{-1})^2=-1$ 可证，把任一复数 $a+b\sqrt{-1}$ 代入任一实系数多项式 $f(x)$，得到的仍是某个复数 $a'+b'\sqrt{-1}$，而两个复数相除仍是复数，所以 R 的这个单代数扩域中的元素的形式是非常简单的。易见，如果 $\alpha\notin F$，则 $F(\alpha)$ 是 F 的真扩域；如果 $\alpha\in F$，则据 F 是域即可证 $F(\alpha)=F$，所以实际上并没有扩大。由此可知，$F(\alpha)=F$ 当且仅当 $\alpha\in F$。这个事实以后常常要用到。

我们进一步考虑这样的问题：一般的单代数扩域 $F(\alpha)$ 中的数可写成怎样的形式？它是否会象在 $C=R(\sqrt{-1})$ 中所见的那样简单呢？我们有以下结果。

定理 3·2 （单代数扩域结构定理）设 α 是域 F 上代数元，α 在 F 上的最小多项式为 $p(x)$，$\deg p(x)=n$，则

$$F(\alpha)=\left\{\sum_{i=0}^{n-1}a_i\alpha^i \middle| a_i\in F\right\},$$

且 $[F(\alpha):F]=n$。此时称 α 是 F 上 n 次代数元。这说明 $F(\alpha)$ 中任一数都可写成系数属于 F 的 α 的多项式，且次数不超过 $n-1$。

证 首先，任取 $1/g(\alpha)\in F(\alpha)$，这里 $g(x)\in F[x]$，$g(\alpha)\neq 0$。因为 $p(x)$ 是 $F[x]$ 中不可约多项式，$g(\alpha)\neq 0$，$p(\alpha)=0$，必有 $p(x)\nmid g(x)$，所以 $g(x)$ 与 $p(x)$ 必互素，即 $g(x)$ 和 $p(x)$ 的公因式必是 F 中的常数。因此根据定理 1·1 知，必可求出 $u(x)$，$v(x)\in F[x]$ 使 $g(x)u(x)+p(x)v(x)=1$。将 $x=\alpha$ 代入，由 $p(\alpha)=0$ 得到 $g(\alpha)u(\alpha)=1$，所以 $1/g(\alpha)=u(\alpha)$是 α 的多项式。其次，任取 $f(\alpha)/g(\alpha)\in F(\alpha)$，可设 $f(\alpha)/g(\alpha)=f(\alpha)u(\alpha)$。由带余除法可设

$$f(x)u(x)=q(x)p(x)+r(x),$$

这里 $r(x)=0$ 或 $0\leqslant\deg r(x)<\deg p(x)$。再利用 $p(\alpha)=0$，得 $f(\alpha)u(\alpha)=r(\alpha)=\sum_{i=0}^{n-1}a_i\alpha^i$，$a_i\in F$。

要证 $[F(\alpha):F]=n$，只要证明 $1,\alpha,\cdots\cdots,\alpha^{n-1}$ 是 $F(\alpha)$ 中的一个 F-基。可表性前已证明，再证表示法是唯一的。设 $F(\alpha)$ 中某数 x 有两种表示法：

$$x=\sum_{i=0}^{n-1}a_i\alpha^i=\sum_{i=0}^{n-1}b_i\alpha^i,\qquad a_i,b_i\in F.$$

令 $c_i=a_i-b_i$，就有 $\sum_{i=0}^{n-1}c_i\alpha^i=0$。如果存在某个系数 $c_i\neq 0$，

则 α 就是 $F[x]$ 中次数小于 n 的非零多项式 $\sum_{i=0}^{n-1} c_i x^i$ 的根，这与 $p(x)$ 是 α 在 F 上的 n 次最小多项式的假设矛盾，所以所有 $c_i=0$，$a_i=b_i$，即表示法唯一。∎

既然在域 F 上添加一个代数元 α_1 可得到单代数扩域 $F(\alpha_1)$，那末，在 $F(\alpha_1)$ 上再添加一个 $F(\alpha_1)$ 上的代数元 α_2 又可得到 $F(\alpha_1)$ 的单代数扩域 $F(\alpha_1)(\alpha_2)$，我们把它记为 $F(\alpha_1,\alpha_2)$ 。(在本节末将证这个 α_2 也是 F 上代数元)。如此下去，经 n 次后可得到 F 的扩域 $E=F(\alpha_1,\alpha_2,\cdots\cdots,\alpha_n)$，每个 α_i 是 $F(\alpha_1,\cdots\cdots,\alpha_{i-1})$ 上的代数元(也是 F 上代数元)。我们称这个 E 是 F 的**有限次添加代数元扩域**。现在，产生了一个问题：对于给定的 F，可以先添加 α_1，再添加 α_2，得到 $F(\alpha_1,\alpha_2)$，也可以先添加 α_2，再添加 α_1，得到 $F(\alpha_2,\alpha_1)$，那末这两个域是否相等呢？回答是必有等式

$$F(\alpha_1,\alpha_2)=F(\alpha_2,\alpha_1)。$$

这可以这样来证明：由单代数扩域的定义，不难看出 $F(\alpha)$是包含 F 和 α 的最小域，$F(\alpha_1,\alpha_2)$ 和 $F(\alpha_2,\alpha_1)$ 都是包含 F，α_1 和 α_2 的最小域，所以它们一定相等，即这样扩域与添加元的添加次序无关。推而广之，可证 $F(\alpha_1,\cdots,\alpha_n)$ 与 α_i 的添加次序无关：

$$F(\alpha_1,\cdots\cdots,\alpha_n)=F(\alpha_{j_1},\cdots\cdots,\alpha_{j_n}),$$

$j_1j_2\cdots j_n$ 是任一 n 阶排列，且此域中任一数必可写成 $\alpha_1,\cdots\cdots,\alpha_n$ 的有理函数，系数属于 F，即

$$F(\alpha_1,\cdots,\alpha_n)=\left\{\frac{f(\alpha_1,\cdots,\alpha_n)}{g(\alpha_1,\cdots,\alpha_n)}\middle| \begin{array}{l} f(x_1,\cdots,x_n),\ g(x_1,\cdots,x_n)\in \\ F[x_1,\cdots,x_n],\ g(\alpha_1,\cdots,\alpha_n)\neq 0 \end{array}\right\},$$

其中 $F[x_1,\cdots,x_n]$ 表示系数属于 F 的 n 个变元 $x_1,\cdots,x_n$ 的多项式全体。因为每个 $F(\alpha_1,\cdots,\alpha_i)$ 是 $F(\alpha_1,\cdots,\alpha_{i-1})$ 的有限扩域，所以应用定理3·1的次数等式，知 $E=F(\alpha_1,\cdots,\alpha_n)$ 必是 F 的有限扩域。因此，有限次添加代数元扩域必是有限扩域。进一步可证，反过来也真。

定理 3·3　设 E 是 F 的有限扩域，则 E 必是 F 的有限次添加代数元扩域：$E=F(\alpha_1,\alpha_2,\cdots\cdots,\alpha_n)$，$\alpha_i$ 都是 F 上代数元。

证　设 $[E:F]=n$。任取 E 中一个 F-基 $\alpha_1,\alpha_2,\cdots,\alpha_n$，可以证明 $E=F(\alpha_1,\alpha_2,\cdots,\alpha_n)$。事实上，因为所有 $\alpha_i\in E$，$F\subseteq E$，而 E 是域，所以 $F(\alpha_1,\alpha_2,\cdots,\alpha_n)\subseteq E$。反之，由基的定义知，任一 $a\in E$ 必可写成 $a=a_1\alpha_1+a_2\alpha_2+\cdots+a_n\alpha_n$，$a_i\in F$，所以 $a\in F(\alpha_1,\alpha_2,\cdots,\alpha_n)$，即 $E\subseteq F(\alpha_1,\alpha_2,\cdots,\alpha_n)$。于是，必有 $E=F(\alpha_1,\alpha_2\cdots,\alpha_n)$。由 $[E:F]=n$ 知，E 的加法群看作 F 上线性空间时其维数是 n，所以对任一取定的 $1\leqslant i\leqslant n$，E 中 $n+1$ 个数 $1,\alpha_i,\alpha_i^2,\cdots,\alpha_i^n$ 必是 F-线性相关的，即存在不全为 0 的 $a_0,a_1,a_2,\cdots,a_n\in F$ 使

$$a_0+a_1\alpha_i+a_2\alpha_i^2+\cdots\cdots+a_n\alpha_i^n=0,$$

于是 α_i 是 $a_0+a_1x+a_2x^2+\cdots\cdots+a_nx^n\in F[x]$ 的根，α_i 是 F 上代数元．▌

由以上论证可知，有限添加代数元扩域与有限扩域是一回事．在下一节中我们将进一步证明，域 F 的任一有限扩域 E 必是单代数扩域 $E=F(\beta)$，因此 E 中任一数必是 β 的多项式，系数属于 F。这样，单代数扩域的重要性就显示出来了，何况它的结构又非常简单，元素都是一些多项式！

顺便提一下，若 E 是 F 的 n 次扩域，则任一 $a\in E$ 必是

F 上代数元。这是由于 $1, \alpha, \alpha^2, \cdots, \alpha^n$ 这 $n+1$ 个数必是 F-线性相关的缘故，所以 F 上有限添加代数元扩域 $E=F(\alpha_1, \alpha_2, \cdots, \alpha_n)$ 中每个 α_i 都是 F 上代数元。

在以下两节中，我们要讨论以伽罗瓦的名字命名的扩域和群。伽罗瓦巧妙地把它们沟通了起来，把域的问题变为群的问题，从而提供了解决五大难题的依据和途径。

§4 伽罗瓦扩域

天才数学家高斯在 22 岁时就证明了著名的代数学基本定理："任意一个复系数多项式在复数域中必有根"。设 $f(x)$ 是 n 次多项式。任取它的一个根 r_1，在复数域 C 上必有分解式 $f(x)=(x-r_1)g(x)$，$\deg g(x)=n-1$；但 $g(x)$ 在 C 中也有根 r_2，它也是 $f(x)$ 的根，故有 $f(x)=(x-r_1)(x-r_2)h(x)$；……如此下去，必可得 $f(x)=a(x-r_1)(x-r_2)\cdots\cdots(x-r_n)$，$a$ 是 $f(x)$ 的首项系数。所以 n 次多项式必有 n 个复数根。例如

$$x^4-2=(x-\sqrt[4]{2})(x+\sqrt[4]{2})(x-\sqrt[4]{2}\,i)(x+\sqrt[4]{2}\,i),$$

这里 $i=\sqrt{-1}$，它有四个复数根 $\pm\sqrt[4]{2}$，$\pm\sqrt[4]{2}\,i$。不难想象，对于一个特定的多项式 $f(x)$ 来说，可能存在比复数域 C 小得多的子域 F 已经包含了 $f(x)$ 的所有根，如果一律放在 C 中考虑就显得浪费了，而且也显示不出 $f(x)$ 的特性。例如，在 C 的真子域 $Q(\sqrt[4]{2}, \sqrt[4]{2}\,i)$ 中已经包含了 x^4-2 的四个根（包含 $\sqrt[4]{2}$ 和 $\sqrt[4]{2}\,i$，必包含相反数 $-\sqrt[4]{2}$ 和 $-\sqrt[4]{2}\,i$）。进一步，任意一个包含 x^4-2 的所有根的域必定包含 Q 和

$\pm\sqrt[4]{2}$，$\pm\sqrt[4]{2}i$，因而必定是 $Q(\sqrt[4]{2},\sqrt[4]{2}i)$ 的扩域。所以 $Q(\sqrt[4]{2},\sqrt[4]{2}i)$ 是包含 x^4-2 的所有根的最小域。同理，包含 x^2+1 的所有根的最小域是 $Q(\sqrt{-1})$，它也是复数域$C=R(\sqrt{-1})$的真子域。

定义 4·1　设 $f(x)$ 是系数属于域 F 的多项式。F 的包含 $f(x)$ 的所有根的最小扩域E称为 $f(x)$ 在F上的**分裂域**。

这里“分裂”的含义指的是，$f(x)$ 能在这个域中分解成一次因子的乘积。关于多项式的分裂域，我们要强调指出以下两点。首先，对于给定的 $f(x)\in F[x]$，尽管它的根 $r_1,r_2,\cdots\cdots,r_n$ 未必知道，但总是客观存在的，而且都是 F 上代数元。把它们统统加到域 F 上，得到 F 的有限添加代数元扩域 $E=F(r_1,r_2,\cdots\cdots,r_n)$，它也是客观存在的域，而且是 F 的有限扩域。我们应该承认客观存在的东西，即使它是未知的，这丝毫也不影响我们作理论上的推导，从而得出正确的结论。易见，把 $f(x)\in F[x]$ 的所有根添加到 F 上去所得到的域 E 就是 $f(x)$ 在 F 上的分裂域。因此，有时候也把分裂域称为**根域**。其次，若 $f(x)\in F[x]$，F' 是 F 的扩域，当然有 $f(x)\in F'[x]$。如果 $f(x)$ 的全体根为 $r_1,r_2,\cdots\cdots,r_n$，则 $f(x)$ 在 F 上的分裂域为 $F(r_1,r_2,\cdots\cdots,r_n)$。同一个 $f(x)$ 在F' 上的分裂域为 $F'(r_1,r_2,\cdots\cdots,r_n)$。一般来说，这两个域未必相等：$F(r_1,\cdots,r_n)\subseteq F'(r_1,\cdots,r_n)$。因此，说到分裂域，应明确指明是在哪个域上的分裂域，仅说 $f(x)$ 的分裂域是没有意义的。例如，x^4-2 既可看成是 Q 上多项式，又可看成是 R 上和 C 上多项式，它在 Q 上的分裂域是 $Q(\sqrt[4]{2},\sqrt[4]{2}i)$。因为 $\sqrt[4]{2}$ 是实数，而 $R(\sqrt[4]{2})=R$，所以它在 R 上的分裂域是 $R(\sqrt[4]{2},\sqrt[4]{2}i)=R(\sqrt[4]{2}i)$，它在 C 上的分裂域就是 C 本

身。

下面我们给出分裂域的重要例子。

例 1 $f(x)=x^n-1$ 可以看成任一域 F 上的多项式。它的任一根称为 n 次单位根。易见，有且仅有 n 个两两不同的 n 次单位根

$$\omega_k=\cos k\theta+\sqrt{-1}\sin k\theta,$$

这里，$\theta=\dfrac{2\pi}{n}$，$k=1,2,\cdots,n$，它们是单位圆周上的 n 个等分点（如图）。用复数的逮莫非(De Moivre, 1667～1754)公式易得

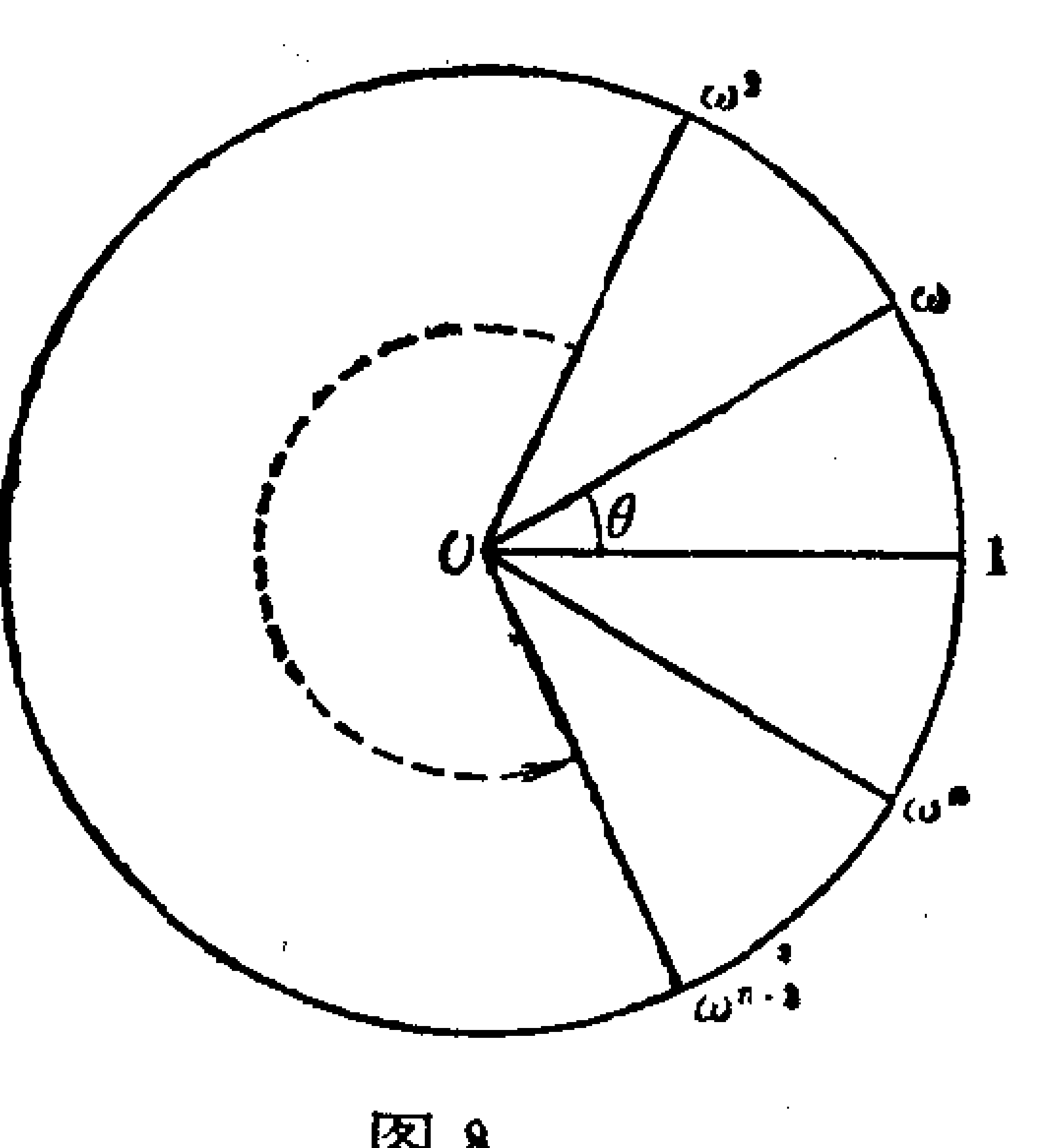


图 8

$$\omega_k=(\cos\theta+\sqrt{-1}\sin\theta)^k=\omega_1^k,$$

所以 n 个 n 次单位根恰成一个 n 阶循环群

$$U_n=\langle\omega_1\rangle,$$

称为 n 次单位根群。例如，

$$U_3=\left\{1,\ \frac{-1+\sqrt{-3}}{2},\ \frac{-1-\sqrt{-3}}{2}\right\}$$

$$=\left\langle\frac{-1+\sqrt{-3}}{2}\right\rangle=\left\langle\frac{-1-\sqrt{-3}}{2}\right\rangle,$$

$$U_4=\{1,\ \sqrt{-1},\ -1,\ -\sqrt{-1}\}$$

$$=\langle\sqrt{-1}\rangle=\langle-\sqrt{-1}\rangle.$$

由于每个根 $\omega_i=\omega_1^i$，所以 x^n-1 在 F 上的分裂域就是 $E=F(\omega_1)$，它是 F 的单代数扩域。当然，这种添加元不一定是唯一的，循环群 U_n 中任一生成元都可作为此单代数扩域的添加元。n 阶循环群 $U_n=\langle\omega_1\rangle$ 中某元 ω_1^k 是生成元，当且仅当它是 n 阶元，当且仅当 $(k,n)=1$，即 k 与 n 互素，它们的最大公因数是 1。这种阶是 n 的 n 次单位根称为 n **次本原根**，共有 $\varphi(n)$ 个(见第 40 页)。若 p 是素数，任一不是 1 的 p 次单位根必是 p 次本原根。例如，3 个 3 次单位根 1，$-\frac{1}{2}+\frac{\sqrt{-3}}{2}$，$-\frac{1}{2}-\frac{\sqrt{-3}}{2}$ 中，有且仅有 2 个 3 次本原根 $-\frac{1}{2}\pm\frac{\sqrt{-3}}{2}$。4 个 4 次单位根 ±1，$\pm\sqrt{-1}$ 中仅有 2 个 4 次本原根 $\pm\sqrt{-1}$，而 -1 是 2 阶元，因而是 2 次本原根。由此可得结论：$f(x)=x^n-1$ 在任一域 F 上的分裂域必是单代数扩域 $E=F(\omega)$，这里 ω 是任一 n 次本原根。现在讨论扩域次数 $[E:F]$。因为

$$x^n-1=(x-1)(x^{n-1}+x^{n-2}+\cdots\cdots+x+1),$$

任一 n 次本原根 ω 必是 $g(x)=x^{n-1}+x^{n-2}+\cdots\cdots+x+1$ 的根。由于 $g(x)$ 在 $F[x]$ 中未必是不可约的，因而未必是 ω 在 F 上的最小多项式，所以 $[F(\omega):F]\leqslant n-1$，其中等号未必成立。例如

$$x^4-1=(x-1)(x+1)(x^2+1).$$

任取 4 次本原根 i，就有 $[F(i):F]=2<3$。如果取系数域为有理数域 Q，则可断定 $[Q(\omega):Q]=\varphi(n)$，这里 ω 是任一 n 次本原根。其根据是，可以证明，由 $\varphi(n)$ 个 n 次本原根（不妨设为 $\omega_1,\omega_2,\cdots\cdots,\omega_{\varphi(n)}$）确定的 $\varphi(n)$ 次多项式

$$\Phi_n(x)=\prod_{i=1}^{\varphi(n)}(x-\omega_i)$$

必是 Q 上的不可约多项式，而且它就是任一 n 次本原根在 Q 上的最小多项式.（证明略）。特别地，对素数 p 次本原根 ω 必有 $[Q(\omega):Q]=\varphi(p)=p-1$。

例 2　设 a 是某域 F 中取定的一个数，则可验证 $f(x)=x^n-a$ 的 n 个根是 $\sqrt[n]{a}$，$\omega\sqrt[n]{a}$，$\omega^2\cdot\sqrt[n]{a}$，……，$\omega^{n-1}\cdot\sqrt[n]{a}$，这里 ω 是任一 n 次本原根。因此，$f(x)$ 在 F 上的分裂域为

$$F(\sqrt[n]{a},\ \omega\cdot\sqrt[n]{a},\ \omega^2\cdot\sqrt[n]{a},\ \cdots,\ \omega^{n-1}\cdot\sqrt[n]{a})=F(\sqrt[n]{a},\omega).$$

这个等式可以这样来证明：因为右边这个域包含了 $\sqrt[n]{a}$ 和 ω，由域中乘法封闭性知，它必包含所有根 $\omega^i\cdot\sqrt[n]{a}$（$i=0,1,\cdots\cdots,n-1$），因而包含左边这个域。反之，因为左边这个域包含 $\sqrt[n]{a}$ 和 $\omega\cdot\sqrt[n]{a}$，所以必包含 $\omega\cdot\sqrt[n]{a}/\sqrt[n]{a}=\omega$，因而包含右边这个域。因此，这两个域相等。

利用分裂域的概念可以证明如下重要而又漂亮的结论。

定理 4·1　域 F 的任一有限扩域 E 必是单代数扩域。

证　先考虑添加两个代数元的情形。设 $E=F(\alpha,\beta)$，F 上的代数元 α 和 β 在 F 上的最小多项式分别是 $f(x)$ 和 $g(x)$。考虑它们的乘积多项式 $f(x)g(x)$ 在 E 上的分裂域 K，则在 $K[x]$ 中有

$$f(x)=(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_m),\ \alpha_1=\alpha,\ \forall\alpha_i\in K,$$

$$g(x)=(x-\beta_1)(x-\beta_2)\cdots(x-\beta_n),\ \beta_1=\beta,\ \forall\beta_i\in K.$$

在 F 中任意取定某个非零数 d 使

$$d\neq\frac{\alpha-\alpha_i}{\beta_j-\beta},\quad\forall i=2,\cdots,m;\ \forall j=2,\cdots,n. \tag{1}$$

易见，右边这种复数最多有 $(m-1)(n-1)$ 个，而 F 是无限域，所以这种 d 必可取到。(尽可能取 $d=1$。)令

$$\theta=\alpha+d\beta,$$

则由 d 的取法知

$$\alpha_i+d\beta_j\neq\theta,\quad \theta-d\beta_j\neq\alpha_i,\ \forall\begin{matrix}i=2,\cdots m,\\ j=2,\cdots n.\end{matrix}$$

现在可以证明 $F(\alpha,\beta)=F(\theta)$。首先，由 $\theta=\alpha+d\beta$ 和 $d\in F$ 知，$F(\theta)\subseteq F(\alpha,\beta)$。为了证明反向包含关系也成立，我们考虑系数在域 $F(\theta)$ 中的多项式

$$h(x)=f(\theta-dx)\in F(\theta)[x],$$

这里 $f(\theta-dx)$ 表示把 $f(x)$ 中的变量 x 统统换成 $\theta-dx$ 得到的新多项式，那末有 $h(\beta)=f(\theta-d\beta)=f(\alpha)=0$。这说明 β 是 $g(x)$ 和 $h(x)$ 的公共根。进一步，对 $g(x)$ 的其它根 β_2，……，β_n，有 $h(\beta_j)=f(\theta-d\beta_j)$。但已知 $\alpha_1,\alpha_2,\cdots\cdots,\alpha_m$ 是 $f(x)$ 的仅有的根，且 $\theta-d\beta_j$ 与任一 α_i 都不等，所以 $h(\beta_j)\neq0$，$2\leqslant j\leqslant n$。这说明了 β 是 $g(x)$ 和 $h(x)$ 唯一的公共根，$x-\beta$ 就是 $g(x)$ 和 $h(x)$ 的最高公因式。我们回忆一下在§1中所讲的多项式的带余除法。设 $g(x)=q(x)h(x)+r(x)$。因为 $g(x)$ 和 $h(x)$ 的公共系数域是 $F(\theta)$，所以 $q(x)$ 和 $r(x)$ 也是 $F(\theta)$ 上的多项式，而 $g(x)$ 和 $h(x)$ 的最高公因式是用辗转相除法求得的，所以 $x-\beta$ 的系数必定属于公共的系数域 $F(\theta)$，这说明 $\beta\in F(\theta)$，所以 $\alpha=\theta-d\beta\in F(\theta)$，又有 $F(\alpha,\beta)\subseteq F(\theta)$。于是 $F(\alpha,\beta)=F(\theta)=F(\alpha+d\beta)$。

既然两个添加元能换成一个，则

$$\begin{aligned}F(\alpha,\beta,\gamma)&=F(\alpha,\beta)(\gamma)=F(\theta)(\gamma)\\&=F(\theta,\gamma)=F(\delta).\end{aligned}$$

更一般地，F 的有限扩域 E 必是有限添加代数元扩域 $E=F(\alpha_1,\alpha_2,\cdots\cdots,\alpha_n)$，因而必是单代数扩域 $E=F(\beta)$。▌

这就告诉了我们一个很有趣的事实：若对 α 和 β 能取到 $d=1$（这在很多情况下可以取到），则必有 $F(\alpha,\beta)=F(\alpha+\beta)$。例如，$Q(\sqrt{2},\sqrt{3})=Q(\sqrt{2}+\sqrt{3})$，这只要验证一下取 $d=1$ 必能满足条件(1)式即可。

根据这个定理可立刻推得：任一 $f(x)\in F[x]$ 在 F 上的分裂域 E 必是 F 的单代数扩域

$$E=F(r_1,r_2,\cdots\cdots,r_n)=F(\alpha)。$$

尽管这个 α 可能很难具体找出来，但是这个结论已经令人非常满意了！

多项式的分裂域有个很奇特的性质，就是它有某种"正规性"。

定义 4·2 设 K 是 F 的有限扩域。如果 K 满足以下条件：$F[x]$ 中的任一 n 次不可约多项式，或者在 K 中无根，或者 n 个根都在 K 中，则称 K 是 F 的**正规扩域**。

满足这种古怪条件的扩域的确是大量存在的。我们先仿照群的同构来定义域的同构。设 F_1 和 F_2 是两个域。如果存在 F_1 到 F_2 的双射 σ，满足

$$(a+b)^\sigma=a^\sigma+b^\sigma,\ (ab)^\sigma=a^\sigma b^\sigma,\ \forall a,b\in F_1,$$

则称 σ 是 F_1 到 F_2 的同构满射。此时称 F_1 和 F_2 是同构的域，记为 $F_1\overset{\sigma}{\cong}F_2$，同时有 $F_2\overset{\sigma^{-1}}{\cong}F_1$，这里 σ^{-1} 是双射 σ 的逆映射：$\sigma\sigma^{-1}=1_{F_1},\sigma^{-1}\sigma=1_{F_2}$。如果不关心是哪个 σ 时，就记为 $F_1\cong F_2$，$F_2\cong F_1$。例如，Q 的以下两个单代数扩域

$$Q(\sqrt{2})=\{a+b\sqrt{2}\mid a,b\in Q\},$$

$$Q(\sqrt{3})=\{a+b\sqrt{3}\mid a,b\in Q\}$$

是同构的。同构映射可取为

$$\sigma: a+b\sqrt{2}\longrightarrow a+b\sqrt{3}。$$

(读者自己可验证一下)。一般地,若 $g(x)$ 是某域 F 上的 n 次不可约多项式, α 和 β 是 $g(x)$ 的两个根,则

$$F(\alpha)=\left\{\sum_{i=0}^{n-1}a_i\alpha^i \,\middle|\, a_i\in F\right\},$$

$$F(\beta)=\left\{\sum_{i=0}^{n-1}a_i\beta^i \,\middle|\, a_i\in F\right\}$$

必是同构的单代数扩域,同构映射可取为

$$\sigma: \sum_{i=0}^{n-1}a_i\alpha^i\longrightarrow\sum_{i=0}^{n-1}a_i\beta^i,\quad \forall a_i\in F。\tag{2}$$

现在可以证明:

定理 4·2 任一 $f(x)\in F[x]$ 在 F 上的分裂域 E 必是 F 的正规扩域。

证 可设 $E=F(\alpha_1,\alpha_2,\cdots,\alpha_n)$,这里 $f(\alpha_i)=0$。若 $g(x)$ 是 $F[x]$ 中某个不可约多项式,已知它有某个根 $\alpha\in E$。任取 $g(x)$ 的根 β, 要证 $\beta\in E$。由 $\alpha\in E$ 知, $f(x)$ 在 $F(\alpha)$ 上的分裂域是

$$F(\alpha)(\alpha_1,\cdots\cdots,\alpha_n)=F(\alpha_1,\cdots,\alpha_n)(\alpha)=E(\alpha)=E,$$

而 $f(x)$ 在 $F(\beta)$ 上的分裂域

$$F(\beta)(\alpha_1,\cdots\cdots,\alpha_n)=F(\alpha_1,\cdots,\alpha_n)(\beta)=E(\beta)。$$

前已说明 $F(\alpha)\overset{\sigma}{\cong}F(\beta)$, σ 如(2)式所示。因为同一个多项式

在同构的域上的分裂域必是同构的(证明略)，所以$E(\beta)\overset{\sigma}{\cong}E$，而且$\tau|_{F(\alpha)}=\sigma$，这说明域$E(\beta)$的加法群和域$E$的加法群之间存在一个双射$\tau$。因为这两个加法群都是$F$上的有限维线性空间，而且由$\tau|_{F(\alpha)}=\sigma$和(2)式知$\tau$限制在$F$上必是恒等变换，因此这个$\tau$也是这两个线性空间的同构。因为同构的线性空间的维数一定相等，所以$[E(\beta):F]=[E:F]$。但$F\subseteq E\subseteq E(\beta)$，所以必有$E(\beta)=E$，$\beta\in E$。这就证明了$E$是$F$的正规扩域。∎

定义 4·3　域F的任一有限正规扩域K称为F的**伽罗瓦扩域**。

因此，任一多项式在系数域F上的分裂域必是伽罗瓦扩域，任一伽罗瓦扩域必是单代数扩域。伽罗瓦扩域是伽罗瓦理论的主要研究对象之一。

设$E=F(\alpha_1,\alpha_2,\cdots\cdots,\alpha_n)$是$F$的任一有限扩域。一般说来，$E$未必是$F$的正规扩域。能否把$E$扩大成$F$的某个正规扩域呢？设$\alpha_i$在$F$上的最小多项式是$g_i(x)$，$i=1,2,\cdots,n$。令

$$f(x)=g_1(x)g_2(x)\cdots\cdots g_n(x),$$

则这个$f(x)$在F上的分裂域K必是F的正规扩域。可以证明，用这种办法构造出来的扩域K必是F的包含E的最小正规扩域。首先，由所有的$\alpha_i\in K$知$E\subseteq K$。其次，任取F的包含E的正规扩域K'，既然K'包含了$g_i(x)$的一个根α_i(因为$\alpha_i\in E$)，由正规性知，它必包含$g_i(x)$的所有根$(i=1,2,\cdots\cdots,n)$，所以K'必包含$f(x)$在F上的分裂域K。我们把这种K称为E的**正规闭包**。毫无疑问，这种正规闭包是客观存在的，它就是上述$f(x)$在F上的分裂域。还有，如果

$$E=F(\alpha_1,\cdots\cdots,\alpha_n)=F(\beta_1,\cdots\cdots,\beta_m),$$

则由这两个不同的添加元组 $\{\alpha_1,\cdots,\alpha_n\}$ 和 $\{\beta_1,\cdots,\beta_m\}$ 所确定的两个正规闭包虽然未必相同，但必是同构的（证明略）。

最后说明一下以后经常要引用的两个事实。首先，设 $E=F(\alpha_1,\cdots,\alpha_n)$ 是 F 的任一伽罗瓦扩域，α_i 在 F 上的最小多项式是 $g_i(x)(i=1,2,\cdots,n)$。既然 E 是 F 的正规扩域，$\alpha_i\in E$，那么 $g_i(x)$ 的所有根都属于 E。因此，E 就是 $f(x)=g_1(x)\cdot g_2(x)\cdots\cdots g_n(x)$ 在 F 上的分裂域。这说明 F 的任一伽罗瓦扩域必是某个 $f(x)\in F[x]$ 在 F 上的分裂域。其次，设给定三个域

$$F\subseteq K\subseteq E。$$

如果 E 是 F 的伽罗瓦扩域，则 E 必是某个 $f(x)\in F[x]$ 在 F 上的分裂域。当然，这个 $f(x)$ 也可看成是 $K[x]$ 中的元素，但已知 $f(x)$ 的所有根都在 E 中，所以由分裂域的定义知，$f(x)$ 在 K 上的分裂域仍然是这个 E，这说明 E 也是 K 的伽罗瓦扩域。但一般说来，K 未必是 F 的伽罗瓦扩域，因为它未必是 F 的正规扩域。

§5 伽 罗 瓦 群

从本节起，我们把 E 是域 F 的扩域这一件事简记为 E/F，这个记号丝毫没有相除的含义。例如，R/Q，C/R，C/Q 等等都表示扩域。域 E 到 E 自身的同构满射称为 E 的**自同构**。因为群的自同构必把单位元变为单位元，所以域的自同构必把 $(E,+)$ 的单位元 0 变为 0，$(E^*,\cdot)$ 的单位元 1 变为 1，因

而保持整数不变，保持一切有理数不变。这说明任一域 E 的任一自同构 σ 限制在有理数域 Q 上必是恒等变换，即$\sigma|_Q=1_Q$。现在要证明，域 E 的自同构全体关于变换的乘法成群。设 σ 和 τ 是 E 中两个自同构，则对任意 $a,b\in E$，有

$$(a+b)^\sigma=a^\sigma+b^\sigma,\quad (ab)^\sigma=a^\sigma b^\sigma,$$

$$(a+b)^\tau=a^\tau+b^\tau,\quad (ab)^\tau=a^\tau b^\tau,$$

于是根据变换乘法的定义知，对任意 $a,b\in E$ 有

$$(a+b)^{\sigma\tau}=(a^\sigma+b^\sigma)^\tau=a^{\sigma\tau}+b^{\sigma\tau},$$

$$(ab)^{\sigma\tau}=(a^\sigma b^\sigma)^\tau=a^{\sigma\tau}b^{\sigma\tau},$$

即 $\sigma\tau$ 也是 E 的自同构。考虑 σ 的逆变换 σ^{-1}。记 $a^\sigma=\bar{a}$，则 $\bar{a}^{\sigma^{-1}}=a$。任取 $\bar{a},\bar{b}\in E$，可设 $\bar{a}=a^\sigma$，$\bar{b}=b^\sigma$，则 $a=\bar{a}^{\sigma^{-1}}$，$b=\bar{b}^{\sigma^{-1}}$。于是根据

$$\bar{a}+\bar{b}=a^\sigma+b^\sigma=(a+b)^\sigma,\qquad \bar{a}\bar{b}=a^\sigma b^\sigma=(ab)^\sigma$$

得

$$(\bar{a}+\bar{b})^{\sigma^{-1}}=a+b=\bar{a}^{\sigma^{-1}}+\bar{b}^{\sigma^{-1}},$$

$$(\bar{a}\bar{b})^{\sigma^{-1}}=ab=\bar{a}^{\sigma^{-1}}\bar{b}^{\sigma^{-1}},$$

所以 σ^{-1} 也是 E 的自同构。这样就证明了 E 的自同构全体关于变换乘法成群，称为 E 的**自同构群**，记为$\mathrm{Aut}\,E$。这个群是集合 E 上的变换群 T 的子群（见第 25 页）。伽罗瓦理论的妙处就在于考虑如下面所说的一些特殊自同构。设 E 是域 F 的扩域，考虑如下的自同构集合

$$\mathrm{Gal}\,E/F=\{\sigma\,|\,\sigma\in\mathrm{Aut}E,a^\sigma=a,\ \forall a\in F\},$$

其中每一个 σ 都不变 F 中的任意数，即 $\sigma|_F=1_F$。仍据子群

判别定理，可证 Gal E/F 是 Aut E 的子群，称为扩域 E/F 的伽罗瓦群。这里的 Gal 就是 Galois 的头三个字母，不妨读作"伽罗瓦"。在 Gal E/F 中，每个自同构都保持 F 中数不变，故又可称为 F- 自同构，所以 Gal E/F 是由 E 中 F- 自同构全体所成的群。

我们的目标是研究多项式，因此，还要定义多项式的伽罗瓦群。设 F 是任一域，$f(x)\in F[x]$，$f(x)$ 在 F 上的分裂域是 E，则把群 Gal E/F 定义为 $f(x)$ 在 F 上的伽罗瓦群，并记为 G_f。这种由某个多项式 $f(x)$ 确定的伽罗瓦群有一个非常重要而又非常简单的性质：任一 $\sigma\in G_f=\text{Gal}\,E/F$ 必把 $f(x)$ 的根变为根。事实上，设

$$f(x)=a_0+a_1x+\cdots\cdots+a_nx^n,\quad a_i\in F。$$

任取 $f(x)$ 的一个根 α，则 $\alpha\in E$，且

$$a_0+a_1\alpha+\cdots\cdots+a_n\alpha^n=0。$$

任取 $\sigma\in\text{Gal}\,E/F$。因为 σ 是域的自同构，且不变所有的系数 a_i，所以必有

$$a_0+a_1\alpha^\sigma+\cdots\cdots+a_n(\alpha^\sigma)^n=0,$$

这说明 α^σ 也是 $f(x)$ 的根。伽罗瓦也许是由于想到了这一点，才取得了巨大的成功！有时就可利用这一事实确定某些扩域的伽罗瓦群。

例 1 设 $E=F(u)$，$u\notin F$，$u^2=a\in F$。易见，$\{1,u\}$ 是 E 中一个 F- 基，E 中任一数必可写成 $b+cu$，其中 $b,c\in F$。因为 $\pm u$ 是 $f(x)=x^2-a$ 的仅有的两个根，所以 $E=F(u)$ 就是 $f(x)=x^2-a\in F[x]$ 在 F 上的分裂域。任取 $\sigma\in\text{Gal}\,E/F$。因为 σ 必把 $f(x)$ 的根变为根：$u\to\pm u$，所以 Gal E/F 中只有两

个元素：一个是恒等变换，另一个就是

$$\sigma : b+cu \longrightarrow b-cu, \quad b,c\in F.$$

所以 Gal E/F 是 2 阶群 $\langle\sigma\rangle$。

例 2 $E=Q(\sqrt{2},\sqrt{3})$。易见 E 是 $f(x)=(x^2-2)(x^2-3)$ 在 Q 上的分裂域。$[E:Q]=[Q(\sqrt{2},\sqrt{3}):Q(\sqrt{2})][Q(\sqrt{2}):Q]=2\cdot2=4$。$f(x)$ 的 4 个根为$\pm\sqrt{2}$，$\pm\sqrt{3}$。任取 $\sigma\in$ Gal E/Q，它必把 $f(x)$ 的根变为根。因为$\pm\sqrt{2}$是 $g(x)=x^2-2$ 的根，$g(x)$ 的系数也在σ之下不变，σ 必把 $g(x)$ 的根变为根。同理，σ 必把$h(x)=x^2-3$ 的根变为根。所以 Gal E/Q 由 4 个元素组成，我们用表说明如下：

	σ_1	σ_2	σ_3	σ_4
$\sqrt{2}\longrightarrow$	$\sqrt{2}$	$\sqrt{2}$	$-\sqrt{2}$	$-\sqrt{2}$
$-\sqrt{2}\longrightarrow$	$-\sqrt{2}$	$-\sqrt{2}$	$\sqrt{2}$	$\sqrt{2}$
$\sqrt{3}\longrightarrow$	$\sqrt{3}$	$-\sqrt{3}$	$\sqrt{3}$	$-\sqrt{3}$
$-\sqrt{3}\longrightarrow$	$-\sqrt{3}$	$\sqrt{3}$	$-\sqrt{3}$	$\sqrt{3}$

如果把 $f(x)$ 的根$\sqrt{2}$，$-\sqrt{2}$，$\sqrt{3}$，$-\sqrt{3}$依次标为 1，2，3，4，则 σ_1 就是恒等变换(1)，σ_2 是对换(3 4)，σ_3是(1 2)，σ_4 是(1 2)(3 4)，所以 Gal E/Q 就是 S_4 的子群

$$\{(1),(1\ 2),(3\ 4),(1\ 2)(3\ 4)\},$$

可证这个群同构于克莱因四元群K_4。

这个例子已经把多项式 $f(x)$ 的伽罗瓦群与 $f(x)$ 的根的集合上的置换联系起来了，这一点非常重要！另外，它还提醒我们：E 中把 $f(x)$ 的根变为根的变换未必是伽罗瓦群中

的元素。事实上，设 E 中某个变换把 $f(x)=(x^2-2)(x^2-3)$ 的根$\sqrt{2}$变为$\sqrt{3}$，如果它是自同构的话，那末必定把 $2=(\sqrt{2})^2$ 变为$(\sqrt{3})^2=3$，但这是不可能的，因为自同构不变任一有理数。

例 3 求 $f(x)=x^4-2$ 在 Q 上的伽罗瓦群。前已提到 $f(x)$在 Q 上的分裂域是 $E=Q(\sqrt[4]{2},i\cdot\sqrt[4]{2})$，这里 $i=\sqrt{-1}$ 是 4 次本原根。$[E:Q]=[Q(\sqrt[4]{2},i\cdot\sqrt[4]{2}):Q(\sqrt[4]{2})][Q(\sqrt[4]{2}):Q]=2\cdot 4=8$。为书写简单起见，记 $\lambda=\sqrt[4]{2}$，则 $f(x)$ 的 4 个根为 $\pm\lambda$, $\pm i\lambda$。根据把根变为根的性质，可知 G_f 由以下 8 个元素构成：

	σ_1	σ_2	σ_3	σ_4	σ_5	σ_6	σ_7	σ_8
$\lambda\to$	λ	λ	$-\lambda$	$-\lambda$	$i\lambda$	$i\lambda$	$-i\lambda$	$-i\lambda$
$-\lambda\to$	$-\lambda$	$-\lambda$	λ	λ	$-i\lambda$	$-i\lambda$	$i\lambda$	$i\lambda$
$i\lambda\to$	$i\lambda$	$-i\lambda$	$i\lambda$	$-i\lambda$	λ	$-\lambda$	λ	$-\lambda$
$-i\lambda\to$	$-i\lambda$	$i\lambda$	$-i\lambda$	$i\lambda$	$-\lambda$	λ	$-\lambda$	λ

(1)

有兴趣的读者可以验证一下这 8 个变换的确成群。

从上面 3 个例子中，我们发现了一个有趣的事实，即群 $\mathrm{Gal}\,E/F$ 的阶数恰巧就是扩域的次数$[E:F]$。实际上，对于多项式的伽罗瓦群来说，这总是成立的，即有

定理 5·1 设 $f(x)\in F[x]$ 在 F 上的分裂域是 E，则

$$|\mathrm{Gal}\,E/F|=[E:F]。$$

证 记 $G=\mathrm{Gal}\,E/F$，$[E:F]=m$，根据定理 4·1 知必存在 $a\in E$ 使

$$E=F(\alpha)=\left\{\sum_{i=0}^{m-1}a_i\alpha^i \,\middle|\, a_i\in F\right\}.$$

设 α 在 F 上的最小多项式是 $g(x)$，则 $g(x)$ 是 m 次不可约多项式，因而一定没有重根(因为 $(g(x),g'(x))\neq 1$)。设它的 m 个根为 $\alpha_1=\alpha,\alpha_2,\cdots\cdots,\alpha_m$。

首先，对任意取定的根 α_j，$1\leqslant j\leqslant m$，变换

$$\sigma_j:\sum_{i=0}^{m-1}a_i\alpha^i\longrightarrow\sum_{i=0}^{m-1}a_i\alpha_j^i,\ \forall a_i\in F$$

显然是 E 中 F- 自同构，所以 $\sigma_j\in G$，它把 α 变为 α_j。因为 $\sigma_1,\sigma_2,\cdots\cdots,\sigma_m$ 两两互异，所以 $|G|\geqslant m$。进一步，任取 $\sigma\in G$，因为 σ 不变 F 中数且把 $f(x)$ 的根 α 变为某个根 α_j，所以 σ 必是上述某个 σ_j。于是证得 $G=\{\sigma_1,\sigma_2,\cdots,\sigma_m\}$，故 $|G|=m$。▌

下面我们要进一步弄清楚多项式的伽罗瓦群与它的根集上的置换群究竟有什么关系。设 F 是任一域，$f(x)\in F[x]$。一般来说，在 $F[x]$ 中，$f(x)$ 可分解为若干个两两不同的不可约多项式 $p_i(x)$ 的乘积

$$f(x)=p_1^{e_1}(x)p_2^{e_2}(x)\cdots\cdots p_s^{e_s}(x),$$

其中自然数 $e_i\geqslant 1$，即 $f(x)$ 可能有重根，但是对应的

$$f_0(x)=p_1(x)p_2(x)\cdots\cdots p_s(x)$$

却没有重根，而且 $f(x)$ 和 $f_0(x)$ 有相同的根，只不过重数不同罢了！所以 $f(x)$ 和 $f_0(x)$ 在 F 上的分裂域相同，它们的伽罗瓦群也是相同的。这件事情告诉我们，只要讨论无重根多项式的伽罗瓦群就行了！

设 $f(x)$ 是 $F[x]$ 中 n 次无重根多项式，它的根集记为

$$R=\{r_1,r_2,\cdots\cdots,r_n\}。$$

任取 $\sigma\in G_f=\mathrm{Gal}\,E/F$，这里 E 是 $f(x)$ 在 F 上的分裂域。因为 σ 把 $f(x)$ 的根变为根，所以可设

$$r_i^\sigma=r_{j_i},\quad i=1,2,\cdots,n,$$

这里下标写成 j_i 表示它与 i 有关，$1\leqslant j_i\leqslant n$。考虑由根的足标组成的 n 元集 $S=\{1,2,\cdots\cdots,n\}$。每一 $\sigma\in G_f$ 可决定 S 上的一个置换

$$\sigma|_R=\begin{pmatrix}1\cdots\cdots i\cdots\cdots n\\ j_1\cdots\cdots j_i\cdots\cdots j_n\end{pmatrix}\in S_n,$$

这里 $\sigma|_R$ 表示 E 中的自同构 σ 限制在根集 R 上考虑。当然有 $R\subseteq E$，所以 σ 在 R 中有定义。考虑由这种方法确定的 G_f 到 S_n 的映射

$$\eta:\sigma\to\sigma|_R,\quad \forall\sigma\in G_f。$$

显然，不同的 σ 决定不同的 $\sigma|_R$，所以 η 是单射。任取 σ，$\tau\in G_f$。设 $r_i^\sigma=r_{j_i}$，$r_i^\tau=r_{k_i}$，则

$$r_i^{\sigma\tau}=(r_i^\sigma)^\tau=(r_{j_i})^\tau=r_{k_{j_i}},\quad i=1,2,\cdots,n。$$

另一方面，对应的两个置换 $\sigma|_R$ 与 $\tau|_R$ 相乘也有

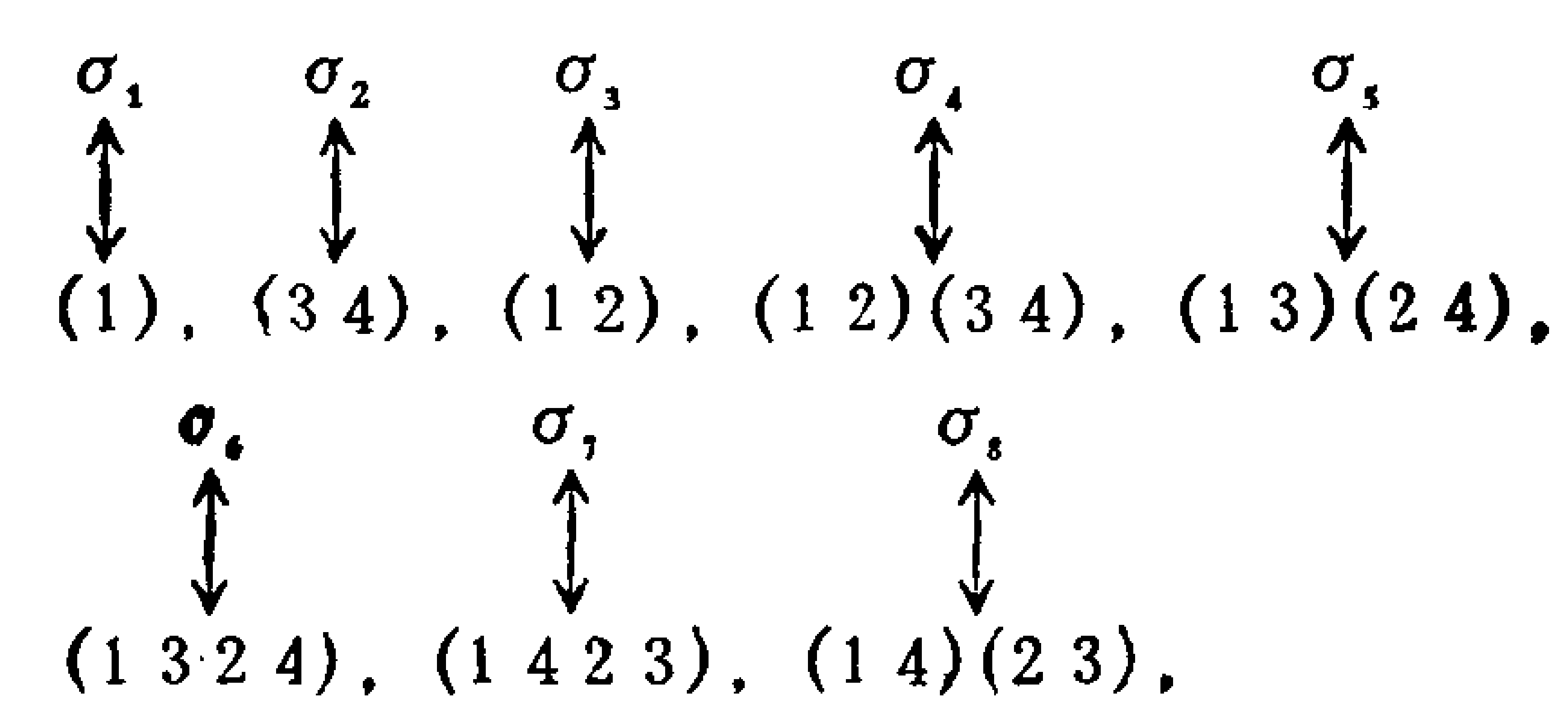
$$\begin{pmatrix}1\cdots i\cdots n\\ j_1\cdots j_i\cdots j_n\end{pmatrix}\begin{pmatrix}j_1\cdots j_i\cdots j_n\\ k_{j_1}\cdots k_{j_i}\cdots k_{j_n}\end{pmatrix}=\begin{pmatrix}1\cdots i\cdots n\\ k_{j_1}\cdots k_{j_i}\cdots k_{j_n}\end{pmatrix},$$

即 $\sigma|_R\cdot\tau|_R=\sigma\tau|_R$，所以 η 是群同构映射，当然它未必是满射，这就证明了。

定理 5·2 设 $f(x)$ 是 $F[x]$ 中 n 次无重根多项式，则 $f(x)$ 在 F 上的伽罗瓦群 G_f 同构于 n 次对称群 S_n 的某个子

群。

例如，在例 1 中，$x^2-a\in F[x]$ 在 F 上的伽罗瓦群恰好同构于 S_2。在例 2 中，$(x^2-2)(x^2-3)$ 在 Q 上的伽罗瓦群同构于 S_4 的子群 $\{(1),(1\ 2),(3\ 4),(1\ 2)(3\ 4)\}$。现在要问：$f(x)=x^4-2$ 在 Q 上的伽罗瓦群 G_f 又同构于 S_4 的哪一个子群呢？它的伽罗瓦群已如表(1)所示。若把 $f(x)$ 的 4 个根 λ，$-\lambda$，$i\lambda$，$-i\lambda$ 依次记为 1，2，3，4，则由表(1)不难看出，G_f 中 8 个元素与 S_4 中一部份元素之间可有如下对应关系：



它们的确构成 S_4 的子群。这个群的几何意义是明显的。作正方形，4 个顶点的编号如右图所示，则上述 8 个置换恰是保持正方形平面位置不变，仅变动顶点的全体置换。例如，以对角线 1 2为轴的翻转就是对换(3 4)，以 1 3 的中点与 2 4的中点的连线为轴的翻转就是(1 3)(2 4)，将正方形逆时针转 90°就是 (1 3 2 4) 等等。

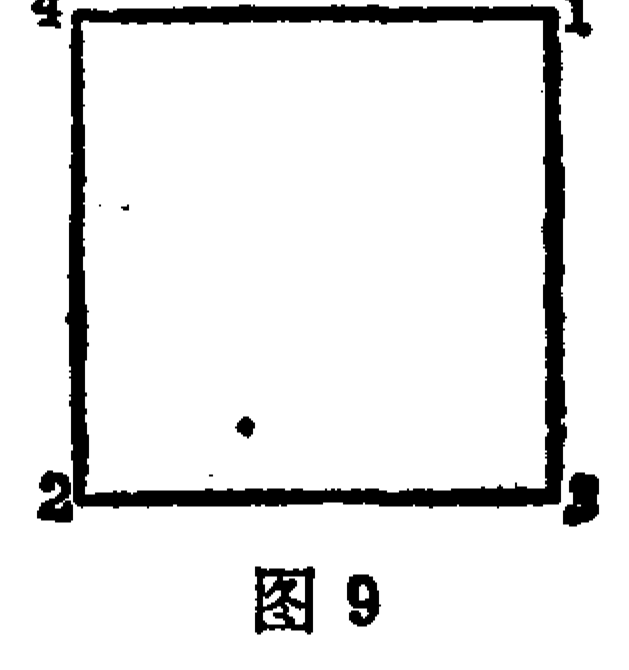


图 9

要确定数字系数代数方程的伽罗瓦群，往往是一件困难而又烦琐的事情。虽然存在一些方法，但由于实用意义不大，而且它与我们在本书中所要解决的问题关系不大，所以我们就不作进一步介绍了，读者也不必花过多的时间去研究它。

现在要问：什么样的 n 次多项式，它的伽罗瓦群恰为 n 次对称群 S_n 呢？我们要寻找的是如下一般代数方程

$$f(x)=a_0x^n+a_1x^{n-1}+\cdots\cdots+a_{n-1}x+a_n=0$$

的求根公式，这里的“一般”两字指的是它的所有系数 a_i 都不是具体的数字而是可取任意值的变元或字母。例如$ax^2+bx+c=0$ 的求根公式是 $x=(-b\pm\sqrt{b^2-4ac})/2a$，这里 a,b,c 都是字母。若有一个具体的二次方程，例如 $x^2+x+1=0$，则可用 $a=b=c=1$ 代入即得 $x=(-1\pm\sqrt{-3})/2$。既然系数都是一些变元，习惯上我们用 t 表示，即我们讨论如下的一般多项式

$$f(x)=x^n-t_1x^{n-1}+t_2x^{n-2}+\cdots\cdots$$
$$+(-1)^kt_kx^{n-k}+\cdots+(-1)^nt_n \qquad (2)$$

的伽罗瓦群。这里，首项系数指定是 1，这丝毫不影响 n 次一般多项式的伽罗瓦群。在其它系数前冠以正负号则纯粹是为了讨论的方便，在以后的讨论过程中读者自然会领会其用意的。说到这里，细心的读者可能会产生一个疑问：既然 $f(x)$ 的系数不是一些具体的数，那末它的系数域是什么呢？我们的回答是域 $F=Q(t_1,t_2,\cdots\cdots,t_n)$，它就是在有理数域 Q 上添加变元 $t_1,t_2,\cdots\cdots,t_n$ 所得的有理分式域(见 §1 末)。但是，前面所讲的扩域都是在某个数域上添加若干个代数元所得的数域，而那些变元 t_i 不可能是有理系数多项式的根，一定不是 Q 上代数元，那末，这又作何理解呢？关于这一点，限于篇幅，我们不准备作进一步解释了。设形如 (2) 的 n 次一般多项式 $f(x)$ 的 n 个根是 $x_1,x_2,\cdots,x_n$，则有

$$f(x)=(x-x_1)(x-x_2)\cdots\cdots(x-x_n)。\qquad (3)$$

比较(2)，(3)两式中的 x 的同次项的系数，且注意到(2)式中各个系数前的正负号，可得 n 个变量的韦达公式：$t_1,t_2,\cdots\cdots,$

t_n 恰好是 $x_1, x_2, \cdots\cdots, x_n$ 的 n 个初等对称多项式。

$$t_1 = \sum x_i = x_1 + x_2 + \cdots + x_n,$$

$$t_2 = \sum_{1 \leqslant i_1 < i_2 \leqslant n} x_{i_1} x_{i_2} = x_1 x_2 + \cdots + x_1 x_n$$
$$+ x_2 x_3 + \cdots + x_{n-1} x_n,$$

$$\cdots\cdots\cdots\cdots\cdots\cdots$$

$$t_k = \sum_{1 \leqslant i_1 < i_2 < \cdots < i_k \leqslant n} x_{i_1} x_{i_2} \cdots x_{i_k}, \tag{4}$$

$$\cdots\cdots\cdots\cdots\cdots\cdots$$

$$t_n = x_1 x_2 \cdots\cdots x_n,$$

这里，t_k 是所有可能的 k 个 x_i 的乘积之和，不过这 k 个 x_i 的下标必须满足 $1 \leqslant i_1 < i_2 < \cdots < i_k \leqslant n$。（见§1）。于是 $f(x)$ 在 F 上的分裂域为

$$E = F(x_1, \cdots\cdots, x_n) = Q(t_1, \cdots\cdots, t_n)(x_1, \cdots\cdots, x_n)$$
$$= Q(x_1, \cdots\cdots, x_n)。$$

最后一个等号成立，是因为据(4)式可知，每个 t_k 都在 $Q(x_1, \cdots\cdots, x_n)$ 之中。根据伽罗瓦群的定义知，$f(x)$ 在 F 上的伽罗瓦群是

$$G = \mathrm{Gal}\, Q(x_1, \cdots\cdots, x_n)/Q(t_1, \cdots\cdots, t_n)。 \tag{5}$$

任取 $\sigma \in G$，则 σ 不变 $f(x)$ 的系数 $t_1, \cdots\cdots, t_n$，因而把 $f(x)$ 的根 x_i 变为 $x_{i'}$，所以 σ 在 $f(x)$ 的根集 $R = \{x_1, \cdots, x_n\}$ 上诱导出一个置换 $\sigma' = \sigma|_R \in S_n$。反之，任取

$$\sigma' = \begin{pmatrix} 1 \cdots\cdots i \cdots\cdots n \\ j_1 \cdots\cdots j_i \cdots\cdots j_n \end{pmatrix} \in S_n.$$

考虑按如下规定

$$\begin{cases} x_i \longrightarrow x_{j_i}, & i=1,2,\cdots n, \quad j_i = i^{\sigma'}, \\ r \longrightarrow r, & \forall r \in Q, \end{cases}$$

所确定的 $Q(x_1,\cdots,x_n)$ 的自同构 σ，即

$$\frac{f(x_1,\cdots,x_i,\cdots,x_n)}{g(x_1,\cdots,x_i,\cdots,x_n)} \xrightarrow{\sigma} \frac{f(x_{j_1},\cdots,x_{j_i},\cdots,x_{j_n})}{g(x_{j_1},\cdots,x_{j_i},\cdots,x_{j_n})},$$

即 σ 不变 f 和 g 的系数，把 x_i 变为 x_{j_i}，且保持域中运算。可以证明 $\sigma \in G$。事实上，按 σ 的构造方法知 σ 不变任一有理数。因为任一 t_k 是 $x_1,\cdots\cdots,x_n$ 的初等对称多项式，系数都是1，所以任一 t_k 必在 σ' 之下不变。再据 $\sigma' = \sigma|_R$ 而 R 是 $f(x)$ 的根集，知 t_k 必在 σ 之下不变，所以 $\sigma \in \mathrm{Gal}\, Q(x_1,\cdots\cdots,x_n)/Q(t_1,\cdots\cdots,t_n)=G$。既然，任一 $\sigma \in G$ 必诱导出某个 $\sigma' = \sigma|_R \in S_n$，根据任一 $\sigma' \in S_n$ 又可构造出某个 $\sigma \in G$ 使 $\sigma|_R = \sigma'$，且 $\sigma \to \sigma'$ 是 G 到 S_n 的同构满射，这就得到了我们盼望已久的结论：

定理 5·3 n 次一般多项式的伽罗瓦群同构于 n 次对称群 S_n。

因为当 $n \geqslant 5$ 时，S_n 不是可解群，所以次数高于四的一般多项式的伽罗瓦群不是可解群。这个结论非常重要，是使伽罗瓦理论获得巨大成功的关键所在。

§6 基 本 定 理

学习好比登山。学到这里，读者可能感到有些累了，不妨稍作休整，回忆一下伽罗瓦扩域和伽罗瓦群的概念和主要结果，然后准备攀登伽罗瓦理论的顶峰—伽罗瓦扩域基本定理。可以这样说，整个伽罗瓦理论的核心就是这个基本定理。学完了这一节，你就渡过了主要难关，剩下的仅是一些应用了！

在上一节中已经说过，对域 E 的任一子域 F，可唯一确定 E 的自同构群 $\mathrm{Aut}\,E$ 的一个子群

$$\mathrm{Gal}\,E/F=\{\eta\,|\,\eta\in\mathrm{Aut}E,\ a^{\eta}=a,\ \forall a\in F\},$$

它就是扩域 E/F 的伽罗瓦群。把 E 的子域全体记为 $\widetilde{F}$，$\mathrm{Aut}E$ 的子群全体记为 $\widetilde{G}$，这样就产生了一个从 $\widetilde{F}$ 到 $\widetilde{G}$ 的映射

$$\sigma\ :\ F\longrightarrow\mathrm{Gal}\,E/F。$$

我们把这一件事用下图表示：

$$\begin{array}{ccc} E & \supseteq & F \\ & & \sigma\big\downarrow \\ \mathrm{Aut}\,E & \geqslant & \mathrm{Gal}\,E/F \end{array}$$

反过来，设 E 是任一给定的域。对 $\mathrm{Aut}\,E$ 的任一子群 G，可确定 E 的如下一个子集

$$\mathrm{Inv}\,G=\{a\,|\,a\in E,\ a^{\eta}=a,\ \forall\eta\in G\},$$

它由所有在 G 中任一元素之下都不变值的 E 中的数组成。

因为两个不变数的和、差、积以及非零不变数的倒数仍是不变数，所以 $\mathrm{Inv}\,G$ 是 E 的子域，称为 G 的不变子域。这样又可产生一个从 $\widetilde{G}$ 到 $\widetilde{F}$ 的映射

$$\tau: G \longrightarrow \mathrm{Inv}\,G.$$

这也可用下图表示：

$$\begin{array}{c} E \supseteq \mathrm{Inv}\,G \\ \tau\uparrow \\ \mathrm{Aut}\,E \geqslant G \end{array}$$

我们把 σ 和 τ 称为两个伽罗瓦映射。

人们很自然地会提出如下问题：给定 E 的子域 F，可得到 $\mathrm{Aut}\,E$ 的子群 $G=\mathrm{Gal}\,E/F$，对于这个子群 G，又可得到 E 的子域 $F'=\mathrm{Inv}\,G=\mathrm{Inv}\,(\mathrm{Gal}\,E/F)$，那末 F 和 F' 之间有什么关系？类似地可问：给定 $\mathrm{Aut}\,E$ 的子群 G，可得到 E 的子域 $F=\mathrm{Inv}\,G$，对于这个子域 F，又可得到 $\mathrm{Aut}\,E$ 的子群 $G'=\mathrm{Gal}\,E/F=\mathrm{Gal}(E/\mathrm{Inv}\,G)$。$G$ 和 G' 有什么关系？一些初步的结论是

定理 6·1 伽罗瓦映射有如下基本性质：

（Ⅰ）$\mathrm{Inv}(\mathrm{Gal}\,E/F)\supseteq F$，

（Ⅱ）若 $F_1\supseteq F_2$，则 $\mathrm{Gal}\,E/F_1\subseteq \mathrm{Gal}\,E/F_2$，

（Ⅲ）$\mathrm{Gal}(E/\mathrm{Inv}\,G)\supseteq G$，

（Ⅳ）若 $G_1\supseteq G_2$，则 $\mathrm{Inv}\,G_1\subseteq \mathrm{Inv}\,G_2$。

这里 F_1，F_2 和 F 都是 E 的子域，G_1，G_2 和 G 都是 $\mathrm{Aut}\,E$ 的子群。

证 （Ⅰ）任取 $a\in F$。由 $\mathrm{Gal}\,E/F$ 的定义知 a 必在 $\mathrm{Gal}\,E/F$ 中任一元素之下不变，所以 a 必属于 $\mathrm{Gal}\,E/F$ 的不变子

域 $\text{Inv}(\text{Gal}\,E/F)$。

（Ⅱ）任取 $\eta\in\text{Gal}\,E/F_1$。η 不变 F_1 中所有数，当然不变 F_2 中所有数，所以 $\eta\in\text{Gal}\,E/F_2$。

（Ⅲ）任取 $\eta\in G$。由 $\text{Inv}\,G$ 的定义知 η 不改变子域 $\text{Inv}\,G$ 中的任一数，所以 $\eta\in\text{Gal}(E/\text{Inv}\,G)$。

（Ⅳ）任取 $a\in\text{Inv}\,G_1$。a 在 G_1 中任一元素之下不变，当然在 G_2 中任一元素之下不变，所以 $a\in\text{Inv}\,G_2$。∎

要记住这四个基本性质并不困难，但是对于我们要解决的问题来说，还需要进一步弄清楚：（Ⅰ）和（Ⅲ）中的等式何时成立？（Ⅱ）和（Ⅳ）的逆命题何时成立？我们有

定理 6·2 设 E/F，E/F_1 和 E/F_2 都是伽罗瓦扩域，则

(1) $\text{Inv}(\text{Gal}\,E/F)=F$，

(2) $F_1\supseteq F_2\Longleftrightarrow\text{Gal}\,E/F_1\subseteq\text{Gal}\,E/F_2$。

证 (1)记 $G=\text{Gal}\,E/F$，$F'=\text{Inv}\,G$，要证 $F'=F$。首先，由基本性质（Ⅰ）知 $F'\supseteq F$，对此再用基本性质（Ⅱ）得

$$\text{Gal}\,E/F'\subseteq\text{Gal}\,E/F=G。$$

但是另一方面由基本性质（Ⅲ）又得

$$\text{Gal}\,E/F'=\text{Gal}(E/\text{Inv}\,G)\supseteq G，$$

所以

$$\text{Gal}\,E/F'=G=\text{Gal}\,E/F。\qquad(1)$$

因为 E/F 是伽罗瓦扩域。$F\subseteq F'\subseteq E$，所以 E/F' 也是伽罗瓦扩域，这一点在§4末已证明过了。根据定理5·1得

$$|\text{Gal}\,E/F|=[E:F]，\ |\text{Gal}\,E/F'|=[E:F']。$$

再由(1)式得 $[E:F]=[E:F']$。于是对 $F\subseteq F'\subseteq E$ 运用次数公式立得 $[F':F]=1$，$F'=F$

(2) 必要性就是基本性质(Ⅱ),再证充分性。设 $\mathrm{Gal}\,E/F_1 \subseteq \mathrm{Gal}\,E/F_2$。由基本性质(Ⅳ)知 $\mathrm{Inv}(\mathrm{Gal}\,E/F_1) \supseteq \mathrm{Inv}(\mathrm{Gal}\,E/F_2)$,但 E/F_1、E/F_2 都是伽罗瓦扩域,所以由第一个结论立得 $F_1 \supseteq F_2$。∎

这个定理是沿着子域——子群——子域的路线进行的。反之,沿着子群——子域——子群这一路线也可得到平行的结论。不过我们先要证明一个引理,它是以近代最伟大的代数学家之一阿丁($E \cdot$Artin,1898~1962)的名字命名的。

引理 (阿丁)设 E 是任一域,G 是 $\mathrm{Aut}\,E$ 的任一有限子群,$F=\mathrm{Inv}\,G$,则 $[E:F] \leqslant |G|$。

证 设 $G=\{\eta_1,\eta_2,\cdots\cdots,\eta_n\}$,其中 $\eta_1=1$ 是恒等自同构。如果能够证明 E 中任意 m 个数 $u_1,u_2,\cdots,u_m$,只要 $m>n$,必定 F- 线性相关,则 E 的加法群$(E,+)$作为子域 F 上的线性空间,其维数决不会超过 $n=|G|$,于是 $[E:F] \leqslant n$。记 u_j 在 η_i 下的象是 $a_{ij}=u_j^{\eta_i}$,$i=1,2,\cdots\cdots,n$,$j=1,2,\cdots\cdots,m$。考虑如下包含 n 个方程和 m 个变量的齐次线性方程组

$$\begin{cases} a_{11}x_1+a_{12}x_2+\cdots\cdots+a_{1m}x_m=0 \\ a_{21}x_1+a_{22}x_2+\cdots\cdots+a_{2m}x_m=0 \\ \cdots\cdots\cdots\cdots\cdots\cdots \\ a_{n1}x_1+a_{n2}x_2+\cdots\cdots+a_{nm}x_m=0 \end{cases} \tag{2}$$

我们把它缩写成

$$\sum_{j=1}^{m} a_{ij}x_j=0, \quad i=1,2,\cdots,n.$$

因为变量个数 m 大于方程个数 n,必有 $m-n$ 个自由变量可

任意取值，所以(2)必有非零解，解的每一个分量都是 E 中的数。如果能够证明存在某个非零解 $b=(b_1,b_2,\cdots,b_m)$，其中每个分量 b_j 都是子域 F 中的数，则由(2)中第一个方程(注意到 $a_{1j}=u_j^{\eta_1}=u_j$)可得

$$u_1b_1+u_2b_2+\cdots+u_mb_m=0,$$

这正好说明 $u_1,u_2,\cdots,u_m$ 是 F-线性相关的，引理就可得证。我们这样取定(2)的某个非零解 $b=(b_1,b_2,\cdots\cdots,b_m)$，使得其中所出现的不是 0 的分量 b_j 的个数最少。这种解尽管难以具体确定，但确实是客观存在的，而且有无限多个。对于理论证明来说，这个存在性已经足够了。进一步，还可假设其中 $b_1=1$，否则的话，可适当调整 x_j 的下标使 $b_1\neq0$，再把解 b 的每个分量都除以 b_1 得到的仍是(2)的解，且 $b_1=1$。这样，我们就可取定(2)的某个非零解

$$b=(1,b_2,\cdots\cdots,b_m), \tag{3}$$

它是非零分量个数最少的一个解。下面证明这个解中每个分量必定都是 F 中数。用反证法，如果(3)中存在某个 b_j，例如 $b_2\notin F$。因为 F 由所有在 G 之下不变的那些数组成，既然 b_2 不在 F 中，则至少存在一个 $\eta_k\in G$ 使 $b_2^{\eta_k}\neq b_2$。就把这个域的同构 η_k 作用到等式组

$$\sum_{j=1}^{m}a_{ij}b_j=0,\quad i=1,2,\cdots\cdots,n$$

上得到

$$\sum_{j=1}^{m}a_{ij}^{\eta_k}\,b_j^{\eta_k}=0,\quad i=1,2,\cdots\cdots,n, \tag{4}$$

这里 $a_{ij}^{\eta_k}=u_j^{\eta_i\eta_k}$。但 G 是一个有限群，由群中消去律成立

知，以下两个集合是相等的

$$\{\eta_1\eta_k, \eta_2\eta_k, \cdots\cdots, \eta_n\eta_k\}=\{\eta_1, \eta_2, \cdots\cdots, \eta_n\}.$$

经过适当重排(4)中等式的编号 i（这相当于重排(2)中各方程的位置），可得

$$\sum_{j=1}^{m} a_{lj} b_j^{\eta_k}=0, \quad l=1,2,\cdots,n,$$

这说明

$$b^{\eta_k}=(b_1^{\eta_k}, b_2^{\eta_k}, \cdots\cdots, b_m^{\eta_k}) \tag{5}$$

也是原方程组(2)的解，且 $b_1^{\eta_k}=1^{\eta_k}=1$。把(3)和(5)这两个解相减得到的仍是解

$$b'=(0, b_2', \cdots\cdots, b_m'),$$

其中 $b_j'=b_j-b_j^{\eta_k}$，$j=2,\cdots,m$。因为 $b_2'=b_2-b_2^{\eta_k}\neq 0$，所以 b' 是(2)的非零解。若原来某个 $b_j=0$，则仍有$b_j'=0$。所以 b' 与 b 相比较，所出现的非零分量个数至少减少一个，这与 b 的选择矛盾。这就证明了 b 中各分量都属于 F，$u_1, \cdots\cdots, u_m$ F-线性相关，$[E:F]\leqslant n$。▌

根据阿丁引理可以证明与定理 6·2 平行的一个结论。

定理 6·3　设 E 是域，G，G_1 和 G_2 是 $\mathrm{Aut}\,E$ 的有限子群，则

(1) $\mathrm{Gal}(E/\mathrm{Inv}\,G)=G$，

(2) $G_1\supseteq G_2 \Longleftrightarrow \mathrm{Inv}\,G_1\subseteq \mathrm{Inv}\,G_2$，

证　(1) 记 $F=\mathrm{Inv}\,G$，$G'=\mathrm{Gal}\,E/F$，要证 $G'=G$。如果我们能够证明 E/F 是伽罗瓦扩域，则必有

$$|G'|=|\mathrm{Gal}\,E/F|=[E:F],$$

再由引理知 $[E:F]\leqslant|G|$，所以 $|G'|\leqslant|G|$。但是基本

性质(Ⅲ)又告诉我们 $G'\supseteq G$,且都是有限群,所以必有 $G'=G$。现在我们就来证明 E 是 F 的有限正规扩域。由引理知E是 F 的有限扩域。再证正规性。设 $p(x)$ 是 $F[x]$ 中某个不可约多项式,不失一般性,可设它的首项系数是 1。如果它有某个根 $r\in E$,要证它的所有根都属于 E。设

$$G=\{\eta_1,\eta_2,\cdots\cdots,\eta_n\},\quad \eta_1=1。$$

记 $r^{\eta_i}=r_i$, $i=1,2,\cdots\cdots,n$, 必有 $r_1=r$。这 n 个 r_i 中可能有相同的,去掉那些重复的,不妨设前 m 个 r_i 两两不同,$m\leqslant n$,则

$$g(x)=\prod_{i=1}^{m}(x-r_i)$$

就是 m 次无重根多项式。由于所有 $r_i\in E$, 所以 $g(x)$ 的系数都属于 E。我们要证明 $g(x)$ 的系数都属于 F(但这并不要求所有的 r_i 都属于 F)。我们知道,$F=\mathrm{Inv}G$ 这件事情说明 E 中某数属于 F 当且仅当它在 G 中任一元素之下不变。现在任取 $\eta\in G$,规定 $x^\eta=x$, 这是为了把域 E 的自同构 η 扩展成 $E[x]$ 中的自同构,就是保持多项式加法和乘法的双射,我们仍用 η 表示它,则

$$\big(g(x)\big)^\eta=\prod_{i=1}^{m}(x-r_i^\eta),$$

因为 η 是双射,且任一 $r_i^\eta=r^{\eta_i\eta}$, $1\leqslant i\leqslant n$ 仍是 $r_1,r_2,\cdots\cdots,r_m$ 这 m 个数中某一个,且两两不同, 所以以下两个集合相等

$$\{r_1,r_2,\cdots\cdots,r_m\}=\{r_1^\eta,r_2^\eta,\cdots\cdots,r_m^\eta\},$$

于是

$$\big(g(x)\big)^\eta=\prod_{i=1}^{m}(x-r_i)=g(x),$$

这说明 $g(x)$ 的系数在任一 $\sigma\in G$ 之下不变，所以 $g(x)\in F[x]$。

因为 $p(x)\in F[x]$，而 $F=\mathrm{Inv}\,G$，所以对任一 $1\leqslant i\leqslant m$ 有

$$p(r_i)=p(r^{\eta_i})=(p(r))^{\eta_i}=0,$$

这说明 $g(x)$ 的任一根必是 $p(x)$ 的根。已知 $g(x)$ 无重根，所以在 $F[x]$ 中 $g(x)$ 必整除 $p(x)$，又已知 $p(x)$ 在 $F[x]$ 中不可约，只好 $g(x)=p(x)$，这说明 $p(x)$ 的根就是那些 $r_1,r_2,\cdots,r_m$，且都在 E 中，于是 E 是 F 的正规扩域。

(2) 必要性就是基本性质(Ⅳ)、再证充分性。设 $\mathrm{Inv}G_1\subseteq\mathrm{Inv}G_2$。由基本性质(Ⅱ)知 $\mathrm{Gal}(E/\mathrm{Inv}\,G_1)\supseteq\mathrm{Gal}(E/\mathrm{Inv}\,G_2)$，但 G_1 和 G_2 都是 $\mathrm{Aut}\,E$ 的有限子群，所以由第一个结论即得 $G_1\supseteq G_2$。▌

据此，可以得到一个很实用的结论。

推论 设 E 是域，G 是 $\mathrm{Aut}\,E$ 的有限子群，则 E 必是 $\mathrm{Inv}\,G$ 的伽罗瓦扩域。

现在我们可以讲伽罗瓦扩域的基本定理了。取定某个伽罗瓦扩域 E/F，记 $G=\mathrm{Gal}\,E/F$。考虑以下两个集合

$$S_1=\{H|H\text{ 是 }G\text{ 的子群}\},$$

$$S_2=\{K|K\text{ 是 }E\text{ 的包含 }F\text{ 的子域}\}.$$

伽罗瓦把这两个互不相干的集合沟通起来，很巧妙地在这两者之间建立了某种一一对应关系，这就深入到事物的本质中去了，取得了惊人的成功。利用这种具有很好性质的对应关系，他建立了一些判别准则，这些判别准则可用来判别一个代数方程能否用根号求解和某些平面几何图形能否限用圆规直尺有限次作出。

定理 6·4 （基本定理）设 E/F 是伽罗瓦扩域，$G=\mathrm{Gal}\,E/F$，则有如下结论：

(1) $H\xrightarrow{\sigma}\mathrm{Inv}\,H$ 是 S_1 到 S_2 的双射，

$K\xrightarrow{\tau}\mathrm{Gal}\,E/K$ 是 S_2 到 S_1 的双射。

(2) S_1 与 S_2 之间存在如下伽罗瓦对应：

① $H_1\supseteq H_2\Longleftrightarrow\mathrm{Inv}\,H_1\subseteq\mathrm{Inv}\,H_2$，

② $|H|=[E:\mathrm{Inv}\,H]$，$[G:H]=[\mathrm{Inv}\,H:F]$，

③ H 是 G 的正规子群 $\Longleftrightarrow\mathrm{Inv}\,H$ 是 F 的正规扩域，此时 $\mathrm{Inv}H/F$ 必是伽罗瓦扩域，且

$$\mathrm{Gal}(\mathrm{Inv}\,H/F)\cong G/H。\tag{6}$$

上述主要内容可用图示意如下：

$$\begin{array}{c} F\subseteq \mathrm{Inv}\,H = K\subseteq E \\ \uparrow\sigma \qquad \downarrow\tau \\ G\geqslant H=\mathrm{Gal}\,E/K\geqslant 1 \end{array}$$

这种伽罗瓦对应图含义清楚，容易记忆，因而非常实用。

证 (1) 先证 σ 是双射。任取 $K\in S_2$，即 $F\subseteq K\subseteq E$。因为 E/F 是伽罗瓦扩域，所以 E/K 也是伽罗瓦扩域。令 $H=\mathrm{Gal}\,E/K$。因为 E 中的 K- 自同构必是 F- 自同构，所以 H 是 G 的子群，即 $H\in S_1$。于是由定理 6·2 知

$$\mathrm{Inv}\,H=\mathrm{Inv}\,(\mathrm{Gal}\,E/K)=K，$$

所以 σ 是满射。设对 G 的两个子群 H_1 和 H_2 有 $\mathrm{Inv}\,H_1=\mathrm{Inv}\,H_2$，则由定理6·3知

$$H_1=\mathrm{Gal}\,E/\mathrm{Inv}\,H_1=\mathrm{Gal}\,E/\mathrm{Inv}\,H_2=H_2。$$

于是证得 σ 是双射。再证 τ 是双射。任取 $H\in S_1$。令 $K=\mathrm{Inv}\,H$，

它当然是 E 的子域。因为 F 中数在 G 之下不变，而 H 是 G 的子群，当然在 H 之下不变，所以 $F\subseteq K$，$K\in S_2$。于是由定理 6·3 得

$$\mathrm{Gal}\,E/K=\mathrm{Gal}\,E/\mathrm{Inv}\,H=H,$$

这说明 τ 是满射。如果对 K_1，$K_2\in S_2$ 有 $\mathrm{Gal}\,E/K_1=\mathrm{Gal}\,E/K_2$。因为 E/F 是伽罗瓦扩域，所以 E/K_1 和 E/K_2 都是伽罗瓦扩域。由定理 6·2 得

$$K_1=\mathrm{Inv}\,(\mathrm{Gal}\,E/K_1)=\mathrm{Inv}(\mathrm{Gal}\,E/K_2)=K_2。$$

于是证得 τ 是双射。

（2）①因为 H_1 和 H_2 都是 G 的有限子群，所以由定理 6·3的结论(2)知 $H_1\supseteq H_2\Longleftrightarrow\mathrm{Inv}\,H_1\subseteq\mathrm{Inv}\,H_2$。

② 设 H 是 G 的子群。记 $K=\mathrm{Inv}\,H$。由定理 6·3 得

$$\mathrm{Gal}\,E/K=\mathrm{Gal}\,E/\mathrm{Inv}\,H=H。$$

对伽罗瓦扩域 E/K 和 E/F 用定理 5.1 依次得到

$$|H|=|\mathrm{Gal}\,E/K|=[E:K]=[E:\mathrm{Inv}\,H],$$

$$\begin{aligned}|G|=|\mathrm{Gal}E/F|&=[E:F]=[E:\mathrm{Inv}\,H][\mathrm{Inv}\,H:F]\\&=|H|\cdot[\mathrm{Inv}\,H:F]。\end{aligned}$$

但由拉格朗日定理知 $|G|=|H|\cdot[G:H]$，所以

$$[G:H]=[\mathrm{Inv}\,H:F]。$$

③ 为了引用方便起见，我们先证明以下事实．设 H 是 $G=\mathrm{Gal}\,E/F$ 的任一子群。取 $K=\mathrm{Inv}\,H$．则 $F\subseteq K\subseteq E$。对任一取定的 $\eta\in G$，可确定 E 的一个子集

$$K^\eta=\{k^\eta\mid k\in K\}。$$

它是 K 中所有数在 η 之下的象的全体。要证 K^η 是域。为此，任取 $k_1^\eta, k_2^\eta \in K^\eta$。由 K 是域和 η 是自同构知

$$k_1^\eta \pm k_2^\eta = (k_1 \pm k_2)^\eta,$$

$$k_1^\eta \cdot k_2^\eta = (k_1 \cdot k_2)^\eta,$$

$$(k_1^\eta)^{-1} = (k_1^{-1})^\eta。$$

都仍是 K^η 中数，所以 K^η 是 E 的子域。再由 F 中数在 η 之下不变知 $F \subseteq K^\eta \subseteq E$。可以证明

$$H \lhd G \Longleftrightarrow K^\eta = K, \quad \forall \eta \in G。 \tag{7}$$

设 H 是 G 的正规子群，则对任一确定的 $\eta \in G$，有 $\eta H = H\eta$。这说明对任一 $\xi \in H$，必存在 $\xi' \in H$ 使得 $\eta\xi = \xi'\eta$，所以注意到 $K = \mathrm{Inv}\,H$，可得

$$(k^\eta)^\xi = k^{\eta\xi} = k^{\xi'\eta} = k^\eta, \quad \forall \xi \in H。$$

这说明 $K^\eta \subseteq \mathrm{Inv}\,H = K$。反之，任取 $k \in K$，有

$$(k^{\eta^{-1}})^{\xi'} = k^{\eta^{-1}\xi'} = k^{\xi\eta^{-1}} = k^{\eta^{-1}}, \quad \forall \xi' \in H,$$

所以 $x = k^{\eta^{-1}} \in \mathrm{Inv}\,H = K$，$k = x^\eta \in K^\eta$，又有 $K \subseteq K^\eta$。于是必有 $K^\eta = K$，必要性得证，再证充分性。设对任意 $\eta \in G$ 都有 $K^\eta = K = \mathrm{Inv}\,H$，则对任意 $\xi \in H$，$k \in K$ 有

$$(k^\eta)^{\eta^{-1}\xi\eta} = k^{\xi\eta} = k^\eta,$$

这说明 $K^\eta \subseteq \mathrm{Inv}(\eta^{-1}H\eta)$，这里 $\eta^{-1}H\eta$ 是 H 在 G 中的共轭子群。反之，任取 $x \in \mathrm{Inv}(\eta^{-1}H\eta)$，则

$$x^{\eta^{-1}\xi\eta} = x, \quad (x^{\eta^{-1}})^\xi = x^{\eta^{-1}}, \quad \forall \xi \in H,$$

所以 $k = x^{\eta^{-1}} \in K$，$x = k^\eta \in K^\eta$，于是 $K^\eta = \mathrm{Inv}(\eta^{-1}H\eta)$。但

已知条件是 $K^{\eta}=K=\mathrm{Inv}\,H$. 所以 $\eta^{-1}H\eta=H$, $H\triangleleft G$, 于是(7)式得证。

现在来证明定理中的第③个结论。

必要性：设 H 是 G 的正规子群，记 $K=\mathrm{Inv}\,H$。由(7)式的必要性知 $K^{\eta}=K$, $\forall\eta\in G$, 这说明任一 $\eta\in G$ 必把 K 中数变成 K 中数，所以可把 E 中的每个 F- 自同构 η 看成 K 中的 F- 自同构，即 $\bar{\eta}=\eta|_K\in\mathrm{Gal}\,K/F$，这里 $\eta|_K$ 表示把 η 限制在 K 中考虑，而且 $\eta\xrightarrow{\nu}\bar{\eta}$ 是 $G=\mathrm{Gal}\,E/F$ 到 $\mathrm{Gal}\,K/F$ 的群同态：$\overline{\eta_1\eta_2}=\bar{\eta}_1\cdot\bar{\eta}_2$。记 G 在 ν 之下的象集为 $\bar{G}$，则 $\bar{G}$ 是 $\mathrm{Aut}\,K$ 的有限子群。进一步可证 $\mathrm{Inv}\,\bar{G}=F$。事实上，G 的不变子域是 F，而 $\bar{G}$ 中元素仅仅是 G 中元素在 K 中的限制，所以 $\bar{G}$ 的不变子域必然仍是 F。到此为止，证明了对于域 K 来说，存在 $\mathrm{Aut}\,K$ 的有限子群 $\bar{G}$ 且 $F=\mathrm{Inv}\,\bar{G}$, 于是套用定理6.3的推论(以 K 代 E, 以 $\bar{G}$ 代 G)立得 K 是 F 的伽罗瓦扩域，当然是正规扩域。必要性得证。此时，进一步可证(6)式成立。首先，由 K/F 是伽罗瓦扩域知

$$\mathrm{Gal}\,K/F=\mathrm{Gal}\,K/\mathrm{Inv}\,\bar{G}=\bar{G}。$$

所以上述 ν 实际上是同态满射。把 ν 的核记为

$$H_0=\{\eta\,|\,\eta\in G,\ \bar{\eta}=\eta|_K=1_K \text{ 是 } K \text{ 中恒等变换}\},$$

这说明 K 中任一数必在 H_0 之下不变，即

$$\mathrm{Inv}\,H=K\subseteq\mathrm{Inv}\,H_0,\quad H\supseteq H_0。$$

另一方面，由 $K=\mathrm{Inv}\,H$ 知对任一 $\eta\in H$ 必有 $\bar{\eta}=\eta|_K=1_K$, 所以 $H\subseteq H_0$, 于是 $H_0=H$。根据同态定理得 $G/H\cong\bar{G}$, 这就是(6)式。

充分性，设 $K=\mathrm{Inv}\,H$ 是 F 的正规扩域，要证 $H\triangleleft G$, 只

要证明对任一 $\eta\in G$,必有 $K^{\eta}=K$。任取 $k\in K$。设 k 在 F 上的最小多项式是 $p(x)$。因为任一 $\eta\in G$ 必把 $p(x)$ 的根变为根,所以每个 k^{η}, $\eta\in G$ 仍是 $p(x)$ 的根。但 K 是 F 的正规扩域,由 $k\in K$ 知 $k^{\eta}\in K$, $\forall\eta\in G$,所以 $K^{\eta}\subseteq K$。因为此关系式对任意 $\eta\in G$ 都成立,当然对 η^{-1} 也成立,所以又有 $K^{\eta^{-1}}\subseteq K$。但这就是 $K\subseteq K^{\eta}$,于是必有 $K^{\eta}=K$。所以 H 是 G 的正规子群。∎

第四章　这些难题是怎样解决的

§1　代数方程根号求解

在本节中我们要运用伽罗瓦扩域基本定理建立一个简洁易用的判别准则，用来判定一个代数方程(数字系数或字母系数)是否存在一个求根公式(在这个公式中只用到系数的加减乘除和开方运算)。让我们倒过来看一下，能用根号求解的方程的求根公式有些什么特点？例如，$f(x)=x^2+x-1=0$ 可用根号求解：$x=(-1\pm\sqrt{5})/2$。这说明只要在有理数域 Q 上添加一个 $\sqrt{5}$，在得到的扩域 $Q(\sqrt{5})$ 中就包含了 $f(x)=0$ 的所有根。又如，$f(x)=x^2-x+1=0$ 也可用根号求解：$x=(1\pm\sqrt{-3})/2$，在 $Q(\sqrt{-3})$ 中包含了 $f(x)$ 的所有根。一般地，二次一般多项式 $f(x)=x^2-t_1x+t_2$ 可看成 $F=Q(t_1,t_2)$ 上的多项式。把 $\sqrt{D}=\sqrt{t_1^2-4t_2}$ 添加到 F 上得到的扩域 $F(\sqrt{D})$ 中包含了 $f(x)$ 的所有根 $x=(t_1\pm\sqrt{D})/2$。总之，对于二次多项式必存在一个扩域塔 $F\subset F(\sqrt{D})$，在 $F(\sqrt{D})$ 中可得到它的所有根。因为 $F(\sqrt{D})$ 是 F 上添加一个 F 中某个数 D 的平方根 $\sqrt{D}$ 而得，所以把 $F(\sqrt{D})$ 称为F的**平方根号扩域**，把 $F\subset F(\sqrt{D})$ 称为**平方根塔**，这个塔共有两层。这里的"根"字是根号之意，并非指 $f(x)$ 的根。对于三次、四次

多项式 $f(x)$ 来说，根据第一章中介绍的求根方法可知，一定可以找到 F 的某个适当大的扩域 K，使得 $f(x)$ 的根都在 K 中，而这个 K 是从 F 出发，经过若干次添加前一域中某数的平方根或立方根而得。当然，对应的根塔的层数就不止两层了！再看一个例子。$f(x)=x^5-2$ 的根为 $\lambda,\omega\lambda,\omega^2\lambda,\omega^3\lambda,\omega^4\lambda$，这里 $\lambda=\sqrt[5]{2}$，$\omega=\mathrm{Cos}72^\circ$ 是 5 次本原根。取 $\alpha=18^\circ$，则由 $\mathrm{Sin}\,3\alpha=\mathrm{Cos}\,2\alpha$ 和 $\mathrm{Sin}\,3\alpha=3\,\mathrm{Sin}\,\alpha-4\,\mathrm{Sin}^3\alpha$，$\mathrm{Cos}\,2\alpha=1-2\mathrm{Sin}^2\alpha$ 得 $4\mathrm{Sin}^2\alpha+2\,\mathrm{Sin}\,\alpha-1=0$，故有

$$\mathrm{Sin}18^\circ=\frac{\sqrt{5}-1}{4}=\mathrm{Cos}72^\circ,$$

$$\mathrm{Sin}72^\circ=\frac{1}{4}\sqrt{10+2\sqrt{5}}=\mathrm{Cos}\,18^\circ,$$

于是，

$$\omega=\frac{1}{4}(-1+\sqrt{5}+\sqrt{-10-2\sqrt{5}}),$$

$$\omega^2=\frac{1}{4}\left[-1-\sqrt{5}+\frac{1}{2}(\sqrt{5}-1)\sqrt{-10-2\sqrt{5}}\right],$$

$$\omega^3=\overline{\omega^2}=\frac{1}{4}\left[-1-\sqrt{5}-\frac{1}{2}(\sqrt{5}-1)\sqrt{-10-2\sqrt{5}}\right],$$

$$\omega^4=\overline{\omega}=\frac{1}{4}(-1+\sqrt{5}-\sqrt{-10-2\sqrt{5}}),$$

这里 $\overline{\omega}$ 表示 ω 的共轭复数。这样就可造出一个根塔（由根号扩域所建成的塔）

$$Q\subset Q(\sqrt[5]{2})\subset Q(\sqrt[5]{2},\sqrt{5})$$
$$\subset Q(\sqrt[5]{2},\sqrt{5},\sqrt{-10-2\sqrt{5}})=K,$$

其中相邻两域的扩域次数依次为 5，2，2，而且都是添加一个

根号所得到的扩域。K 中包含了 $f(x)$ 的所有根，所以 $x^5-2=0$ 可用根号求解。

通过上述这些例子可以猜想得到：一个代数方程是否可用根号求解似乎可用上述这种根塔是否存在来刻划。事实的确如此，我们给出如下确切定义。

定义 1·1　设 $f(x)$ 是某一首项系数为 1 的多项式，系数属于某域 F，称 $f(x)=0$ 在 F 上可用根号求解，如果存在 F 的某个扩域 K 满足以下条件：

(1) K 包含了 $f(x)$ 在 F 上的分裂域 E，即 $F\subseteq E\subseteq K$，

(2) 扩域 K/F 有如下根塔①

$$F=F_1\subseteq F_2\subseteq\cdots\cdots\subseteq F_r\subseteq F_{r+1}=K,$$

其中每个 $F_{i+1}=F_i(d_i)$，$d_i^{n_i}=a_i\in F_i$，$i=1,2,\cdots,r$。对应的自然数集 $\{n_1,n_2,\cdots\cdots,n_r\}$ 称为此根塔的根次数集。

用这种条件定义方程可用根号求解是否合理？因为每个 F_{i+1} 是把 $F_i[x]$ 中某个 n_i 次方程 $x^{n_i}-a=0$ 的一个根 $d_i=\sqrt[n_i]{a}$ 添加到 F_i 上而得的单代数扩域，所以 F_{i+1} 中每个数都可表示为 d_i 的多项式，系数属于 F_i，即 F_{i+1} 中的每个数都可由 F_i 中的数经过有限次加减乘除和开 n_i 次方运算得出。因为 $f(x)=0$ 的所有根都在分裂域 E 中，因而也在 K 中，所以 $f(x)=0$ 的每一个根都可利用 $f(x)$ 的系数，经过有限次加减乘除和开根号运算表示，这恰好就是通常所说的方程可用根号求解的含义，因此定义是合理的。

任意取定域 F 中某个数 a，$F(\sqrt[n]{a})$ 称为 F 的根次数是 n 的根号扩域，添加元是 $F[x]$ 中纯多项式 x^n-a 的一个

---

① 这种塔是以 F 为塔基倒着建造的，好比塔在水中的倒影一样。

根。因为它未必是$\sqrt[n]{a}$在 F 上的最小多项式，所以$[F(\sqrt[n]{a}):F]\leqslant n$。例如$\sqrt{-1}$是 $x^4-1=0$ 的根，而$[Q(\sqrt{-1}):Q]=2<4$。根塔是由一串根号扩域建成的。鉴于纯多项式如此重要，就有必要专门来讨论一下了。

定理 1·1　设 n 是某个确定的自然数，域 F 含有 n 次本原根 ω。

(1) 任取 $a\in F$，$a\neq 0$。如果 E 是 $f(x)=x^n-a$ 在 F 上的分裂域，则 $\mathrm{Gal}\,E/F$ 必是 m 阶循环群，$m|n$。

(2) 如果 E 是域 F 的这样一个伽罗瓦扩域，使得 $\mathrm{Gal}\,E/F$ 是 n 阶循环群，则必存在 $d\in E$，使 $d^n=a\in F$，且 $E=F(d)$。

证 (1) 记 $r=\sqrt[n]{a}$，则 $f(x)$ 的根为 $r,\omega r,\omega^2 r,\cdots\cdots,\omega^{n-1}r$。因为 $\omega\in F$，所以 $f(x)$ 在 F 上的分裂域是

$$E=F(\omega,r)=F(r)。$$

这说明 E 中任意一个 F- 自同构（即 $\mathrm{Gal}\,E/F$ 中任意一个元素）是由 r 的象唯一确定的。任取 σ，$\tau\in G=\mathrm{Gal}\,E/F$，它们把 $f(x)$ 的根变为根，可设

$$r^\sigma=\omega^i r,\quad r^\tau=\omega^j r,\quad 0\leqslant i,\ j\leqslant n-1.$$

由 $\omega\in F=\mathrm{Inv}\,G$ 知

$$r^{\sigma\tau}=(\omega^i r)^\tau=\omega^i r^\tau=\omega^{i+j}r.$$

这说明由 $r^\sigma=\omega^i r$ 所确定的映射

$$\eta:\sigma\to\omega^i,\quad \forall\sigma\in G$$

是 G 到 n 次单位根群 $U_n=\langle\omega\rangle$ 的同态映射。进一步，由 $\omega^i=\omega^j\Longleftrightarrow r^\sigma=r^\tau\Longleftrightarrow\sigma=\tau$ 知 η 还是单射，所以 G 同构于$\langle\omega\rangle$ 的某个子群，当然是循环群，而且 $|G|$ 整除 n。

(2) 因为 E 是 F 的伽罗瓦扩域，所以可设 $E=F(\theta)$。据条件知 $G=\mathrm{Gal}\,E/F=\langle\sigma\rangle$，$\sigma$ 是 G 中 n 阶元。把 θ 在 σ^k 作用下的象记为 θ_k：

$$\theta_k=\theta^{\sigma^k},\quad k=0,1,2,\cdots,n-1,\quad \theta_0=\theta。$$

在 E 中取如下 $n-1$ 个数

$$d_1=\theta_0+\theta_1\omega+\theta_2\omega^2+\cdots\cdots+\theta_{n-1}\omega^{n-1},$$

$$d_2=\theta_0^2+\theta_1^2\omega+\theta_2^2\omega^2+\cdots\cdots+\theta_{n-1}^2\omega^{n-1},$$

··················

$$d_i=\theta_0^i+\theta_1^i\omega+\theta_2^i\omega^2+\cdots\cdots+\theta_{n-1}^i\omega^{n-1},\qquad(1)$$

··················

$$d_{n-1}=\theta_0^{n-1}+\theta_1^{n-1}\omega+\theta_2^{n-1}\omega^2+\cdots\cdots+\theta_{n-1}^{n-1}\omega^{n-1}.$$

如果 $d_1,d_2,\cdots,d_{n-1}$ 全为 0，利用 ω 是

$$x^n-1=(x-1)(x^{n-1}+x^{n-2}+\cdots\cdots+x+1)$$

的根，且 $\omega\neq1$，知

$$0=1+\omega+\omega^2+\cdots\cdots\omega^{n-1}。$$

把它放在(1)的前面作为第一个方程，就得到某个含 n 个变量和 n 个方程的齐次线性方程组。因为已知它有非零解

$$(1,\omega,\omega^2,\cdots\cdots,\omega^{n-1}),$$

所以它的系数行列式(是 n 阶范达蒙行列式)

$$V=\prod_{0\leq j<i\leq n-1}(\theta_i-\theta_j)=0。$$

这就是说，至少存在一对 i，j 使 $\theta_i=\theta_j$，即 $\theta^{\sigma^i}=\theta^{\sigma^j}$。但

$E=F(\theta)$，$\mathrm{Gal}\,E/F$ 中元由 θ 的象唯一确定，所以 $\sigma^i=\sigma^j$。由 σ 是 n 阶元且 $0\leqslant j<i\leqslant n-1$ 知这是不可能的。所以 d_1，$d_2,\cdots,d_{n-1}$ 不可能都是 0，至少存在某个 $d_i\neq 0$。记 $d=d_i$，将 $\theta_k=\theta^{\sigma^k}$ 代入这个 d_i 的定义式得

$$d=\theta^i+(\theta^\sigma)^i\omega+(\theta^{\sigma^2})^i\omega^2+\cdots+(\theta^{\sigma^{n-1}})^i\omega^{n-1}。$$

反复利用 $\omega^\sigma=\omega$，$\sigma^n=1$，$\omega^n=1$ 得

$$d^\sigma=\omega^{-1}d,$$

$$(d^2)^\sigma=(d^\sigma)^2=\omega^{-2}d^2,$$

$$\cdots\cdots\cdots\cdots\cdots\cdots$$

$$(d^n)^\sigma=(d^\sigma)^n=\omega^{-n}d^n=d^n。$$

所以，由 $G=\langle\sigma\rangle$ 知，d^n 属于 $F=\mathrm{Inv}\,G$。记 $a=d^n\in F$，于是，剩下来仅需证明 $E=F(\theta)=F(d)$。

首先，由 $d\in E$ 和 $F\subseteq E$ 知，$F(d)\subseteq E=F(\theta)$。进一步，由 $d^\sigma=\omega^{-1}d$ 知，σ 把 $F(d)$ 中数仍变为 $F(d)$ 中数，所以 σ 限制在 $F(d)$ 中就是 $\mathrm{Gal}\,F(d)/F$ 中元素，于是，$G=\langle\sigma\rangle$ 中所有元素限制在 $F(d)$ 中都是 $\mathrm{Gal}\,F(d)/F$ 中的元素。如果 $d^{\sigma^k}=d^{\sigma^l}$，则 $\sigma^k=\sigma^l$，$k=l$，这说明 $\langle\sigma\rangle$ 中 n 个不同的元素限制在 $F(d)$ 中仍是 n 个不同的元素，所以

$$[F(d):F]=|\mathrm{Gal}\,F(d)/F|\geqslant n=[F(\theta):F],$$

（第一个等式是由于 $F(d)/F$ 也是伽罗瓦扩域的缘故）。再据 $F\subseteq F(d)\subseteq F(\theta)$ 得，$F(d)=F(\theta)=E$。∎

这个定理说明了这样一个重要事实：对确定的自然数 n 来说，只要基域 F 含有 n 次本原根，则 F 的根次数是 n 的根号扩域（即 $x^n-a\in F[x]$ 在 F 上的分裂域）的伽罗瓦群必是

m 阶循环群，m 是 n 的某个因子。反之，伽罗瓦群为 n 阶循环群的伽罗瓦扩域必是根次数是 n 的根号扩域。根号扩域的伽罗瓦群与循环群之间竟有着如此密切的关系！而循环群的结构是很清楚的。

要求基域 F 含有某次本原根这一条件确实给建立判别准则带来不少麻烦。如果考虑特殊的纯多项式 $f(x)=x^n-1$，则情况就很好了。

定理 1·2　设 F 是任一域，$f(x)=x^n-1$ 在 F 上的分裂域为 E，则 $\mathrm{Gal}\,E/F$ 必是交换群。

证　在第三章 §4 的例 1 中已经证明了 $E=F(\omega)$，ω是任一 n 次本原根。$f(x)=0$ 的根的全体组成 n 阶循环群 $U_n=\langle\omega\rangle$。任取 $\sigma\in G=\mathrm{Gal}\,F(\omega)/F$。因为 σ 把 $f(x)$ 的根变为根，所以 σ 限制在 U_n 中就是 U_n 的自同构 $\overline{\sigma}=\sigma|_{U_n}$。若用 $\mathrm{Aut}\,U_n$ 表示由 U_n 中的群自同构全体所成的乘法群，则 $\sigma\to\overline{\sigma}$ 是 G 到 $\mathrm{Aut}\,U_n$ 的同构映射，G 同构于 $\mathrm{Aut}\,U_n$ 的某个子群 $\overline{G}$。若能证明 $\mathrm{Aut}\,U_n$ 是交换群，则 $\overline{G}$ 和 G 必是交换群了。任取 ξ，$\eta\in\mathrm{Aut}\,U_n$，可设 $\omega\xrightarrow{\xi}\omega^k$，$\omega\xrightarrow{\eta}\omega^l$，则由

$$\omega\xrightarrow{\xi}\omega^k\xrightarrow{\eta}\omega^{lk},\quad \omega\xrightarrow{\eta}\omega^l\xrightarrow{\xi}\omega^{kl}。$$

知 $\xi\eta=\eta\xi$，所以 $\mathrm{Aut}\,U_n$ 是交换群。▌

现在可以建立判别准则，以达到我们的第一个目标——代数方程何时可用根号求解。

定理 1·3　（判别准则）设 F 为域，$F[x]$ 中多项式 $f(x)$ 在 F 上的伽罗瓦群为 G_f，则 $f(x)=0$ 可用根号求解$\Longleftrightarrow G_f$ 是可解群。

证　必要性。设 $f(x)=0$ 可用根号求解，则据定义知必存在 F 的某个扩域 K，它有根塔

$$F=F_1\subseteq F_2\subseteq\cdots\cdots\subseteq F_r\subseteq F_{r+1}=K, \tag{2}$$

$$F_{i+1}=F_i(d_i),\ d_i^{n_i}\in F_i,\ i=1,2,\cdots\cdots,r,$$

且 K 包含 $f(x)$ 在 F 上的分裂域 E。这个 K 未必是 F 的伽罗瓦扩域,无法套用基本定理。但是 K 的正规闭包 $\overline{K}$ 必是 F 的伽罗瓦扩域,(见第 97 页)。而且可根据 K/F 的根塔(2),构造出 $\overline{K}/F$ 的根塔,且仍有 $F\subseteq E\subseteq K\subseteq\overline{K}$。新根塔的层次可能增加,但不会产生新的根次数,只不过把原有的某些根次数重复几次罢了!(证明略)因此,我们不妨假设(2)中的 K 是 F 的伽罗瓦扩域。

设根塔(2)中所有根次数 $n_1,n_2,\cdots\cdots,n_r$ 的最小公倍数是 n。任意取定一个 n 次本原根 z。由于定理 1.1 中要求基域中含有某次本原根,我们干脆先把 z 添加到(2)中每个域上去,即令

$$K_i=F_i(z),\quad i=1,2,\cdots,r,r+1,$$

那末从根塔(2)又可得到 $K(z)/F$ 的一个根塔

$$F=K_0\subseteq K_1\subseteq K_2\subseteq\cdots\cdots\subseteq K_r\subseteq K(z)=K_{r+1},$$

这里

$$K_1=F(z)=K_0(z),$$

$$K_{i+1}=F_{i+1}(z)=F_i(z,d_i)=K_i(d_i),$$

$$d_i^{n_i}\in F_i\subseteq K_i,\ i=1,2,\cdots\cdots r。$$

因为 K 是 F 的伽罗瓦扩域,所以 K 必是某个 $g(x)\in F[x]$ 在 F 上的分裂域。因为 z 是 n 次本原根, $x^n-1=0$ 的根都是 z 的方幂,所以 $K(z)$ 就是 $g(x)(x^n-1)\in F[x]$ 在 F 上的分裂域,因而 $K(z)$ 必是 F 的伽罗瓦扩域, $K(z)$ 也是每个 K_i 的

伽罗瓦扩域，$i=0,1,\cdots\cdots r$。记

$$H_i=\mathrm{Gal}\,K(z)/K_i,$$

则 $K_i=\mathrm{Inv}\,H_i$，$i=0,1,\cdots\cdots,r$。现在考虑伽罗瓦对应图

$$\begin{array}{ccccccccccc}
F=K_0 & \subseteq\cdots\cdots\subseteq & K_i & \subseteq & K_{i+1} & \subseteq\cdots\cdots\subseteq & K_r & \subseteq & K_{r+1}=K(z) \\
\updownarrow & & \updownarrow & & \updownarrow & & \updownarrow & & \updownarrow \\
H_0 & \geqslant\cdots\cdots\geqslant & H_i & \geqslant & H_{i+1} & \geqslant\cdots\cdots\geqslant & H_r & \geqslant & 1
\end{array}$$

这里 1 是 H_0 的单位元群。因为 $K_1=F(z)$ 是 x^n-1 在 F 上的分裂域，由定理 1.2 知，$\mathrm{Gal}\,K_1/F$ 是交换群。对于任一 $i(1\leqslant i\leqslant r)$，由于 K_i 中已包含了 n_i 次本原根 $z^{\frac{n}{n_i}}$，而 $K_{i+1}=K_i(d_i)$ 是 $x^{n_i}-d_i^{n_i}\in K_i[x]$ 在 K_i 上的分裂域，由定理 1.1 知，$\mathrm{Gal}\,K_{i+1}/K_i$ 也是交换群。于是应用基本定理，由 K_{i+1}/K_i 是正规扩域知 H_{i+1} 是 H_i 的正规子群，且每个商群因子

$$H_i/H_{i+1}\cong\mathrm{Gal}\,K_{i+1}/K_i$$

都是交换群，所以 $H_0=\mathrm{Gal}\,K(z)/F$ 是可解群。再考虑另一张伽罗瓦对应图

$$\begin{array}{ccccc}
F & \subseteq & E & \subseteq & K(z) \\
\updownarrow & & \updownarrow & & \updownarrow \\
H_0 & \geqslant & \widetilde{H} & \geqslant & 1
\end{array}$$

其中 E 是 $f(x)$ 在 F 上的分裂域，$\widetilde{H}=\mathrm{Gal}\,K(z)/E$。因为 E 是 F 的正规扩域，所以 $\widetilde{H}$ 是 H_0 的正规子群，且 $f(x)$ 的伽罗瓦群

$$G=\mathrm{Gal}\,E/F\cong H_0/\widetilde{H}。$$

因为 H_0 是可解群，所以商群 G 也是可解群。

充分性。设 $f(x)$ 在 F 上的分裂域为 E，$G=\mathrm{Gal}\,E/F$ 是可解群。设 $|G|=n$，则 $[E:F]=n$。任取 n 次本原根 z。为了套用定理 1.1，我们又要把 z 添加到 $F\subseteq E$ 上，得

$$F=F_1\subseteq F_2=F(z)\subseteq K=E(z)。$$

因为 $f(x)$ 在 F_1 上的分裂域是 E，所以 $f(x)$ 在 F_2 上的分裂域就是 $E(z)=K$。现在我们要在 F 上造一个包含 E 的根塔，因为 $F_2=F(z)$ 已经是 F 的根号扩域了，而 K 的确是包含 E 的，所以我们只要造一个从 F_2 到 K 的根塔就行了！这里又要用到一个我们不准备给出证明的事实：（参见右边的扩域图）$H=\mathrm{Gal}\,K/F_2$ 同构于 $G=\mathrm{Gal}\,E/F$ 的某个子群。既然 G 是有限可解群，则 H 也是有限可解群，它必有合成群列

$$H=H_1\rhd H_2\rhd\cdots\cdots\rhd H_r\rhd H_{r+1}=1,$$

其中每个合成因子群 H_i/H_{i+1} 都是素数 p_i 阶循环群，$1\leqslant i\leqslant r$，且 $p_i|n$。因为 K 是 F_2 的伽罗瓦扩域，又可套用基本定理得伽罗瓦对应图

$$\begin{array}{ccccccccc}
H=H_1\rhd\cdots\cdots\rhd & H_i & \rhd & H_{i+1} & \rhd\cdots\cdots\rhd & H_r & \rhd & H_{r+1}=1 \\
\updownarrow & \updownarrow & & \updownarrow & & \updownarrow & & \updownarrow \\
F_2\subseteq\cdots\cdots\subseteq & F_{i+1} & \subseteq & F_{i+2} & \subseteq\cdots\cdots\subseteq & F_{r+1} & \subseteq & F_{r+2}=K
\end{array}$$

必有

$$H_i = \mathrm{Gal}K/F_{i+1},$$

$$\mathrm{Gal}F_{i+2}/F_{i+1} \cong H_i/H_{i+1}, \quad i=1,2,\cdots\cdots r。$$

因为 $F_2=F(z)$ 中已经包含了所有的 p_i 次本原根 $z^{\frac{n}{p_i}}$，而 $\mathrm{Gal}F_{i+2}/F_{i+1}$ 是 p_i 阶循环群，所以套用定理 1.1 知，存在 $d_{i+1} \in F_{i+2}$ 使得

$$F_{i+2}=F_{i+1}(d_{i+1}), \quad d_{i+1}^{p_i} \in F_{i+1}, \quad 1 \leqslant i \leqslant r.$$

于是就得到了所需的根塔

$$F=F_1 \subseteq F_2 \subseteq \cdots\cdots \subseteq F_{r+1} \subseteq F_{r+2}=K,$$

根次数依次为 n, $p_1, p_2, \cdots\cdots, p_r$，且 $K=E(z)$ 包含了 $f(x)$ 在 F 上的分裂域 E，所以 $f(x)=0$ 可用根号求解。▌

证明了这个判别准则后；一切就到了瓜熟蒂落的时候了！既然 n 次一般多项式 $f(x)$ 的伽罗瓦群 G_f 在 $n \geqslant 5$ 时不是可解群，我们也就自然地达到了最终的目标：

定理 1·4 （鲁非尼——阿贝尔）高于四次的一般代数方程不可能用根号求解。

这一结论结束了人们在两百多年里徒劳的努力，在这个意义上来说，四次代数方程的求根公式实在称得上是代数学历史上的一个里程碑。

最后，我们给出伽罗瓦的另一个精彩结果，但是不予证明了。他考虑了一个数字系数代数方程何时可用根号求解的问题。

定理 1·5 设 $f(x)$ 是有理系数的素数 p 次不可约多项式。如果 $f(x)$ 有且仅有一对共轭非实根，则 $f(x)$ 在有理数域 Q 上的伽罗瓦群 G_f 同构于 S_p。因此，当 $p \geqslant 5$ 时，$f(x)=0$ 不能用根号求解。

例如，$f(x)=x^5-1$有两对共轭非实根，所以可以用根号求解。又如，$f(x)=x^5-4x+2$，运用关于多项式的施斗姆(Sturm)定理可以判定，$f(x)$ 有且仅有 3 个实根，所以仅有一对共轭非实根，$f(x)$ 不能用根号求解。

§2 圆规直尺作图

在第一章§2 中已介绍了一些圆规直尺作图的方法，但都不符合规尺作图的要求。为什么这些方法都是犯规的呢？这就要搞清楚圆规直尺的最大功能是什么？也就是用圆规直尺能且仅能作出哪些平面几何图形来？这一切都可用代数语言精确地描述出来。用 W 表示通常的二维欧氏平面。所谓**初等几何图形**指的是能限用圆规直尺经有限步作出的平面几何图形。根据圆规直尺的功能易知，初等几何图形必定是由点、线、圆弧和角度构成的。直线由线上任意两点决定，圆弧由它上面的任意三点决定，角度也由其顶点和两边上各取一点决定，所以归根到底，初等几何图形必可通过点的构作来画出。但是，点是几何概念，无法直接用代数方法处理，因而还需把它们代数化。在欧氏平面上取定某个直角坐标系，则平面上的点 $P=(x,y)$ 与复数 $z=x+iy\ (i=\sqrt{-1})$ 是互相唯一确定的，因此，又可把 W 看成是复平面。这样，就把构作点的问题变为构作复数的问题了。对于复数，也许有可能应用伽罗瓦理论讨论了！我们约定：今后不再注意点和数的形式差别了。

构作任一初等几何图形，必须预先给定某些已知点或数。例如，要用圆规直尺三等分 60^0角。以顶点O为圆心，以 1 为

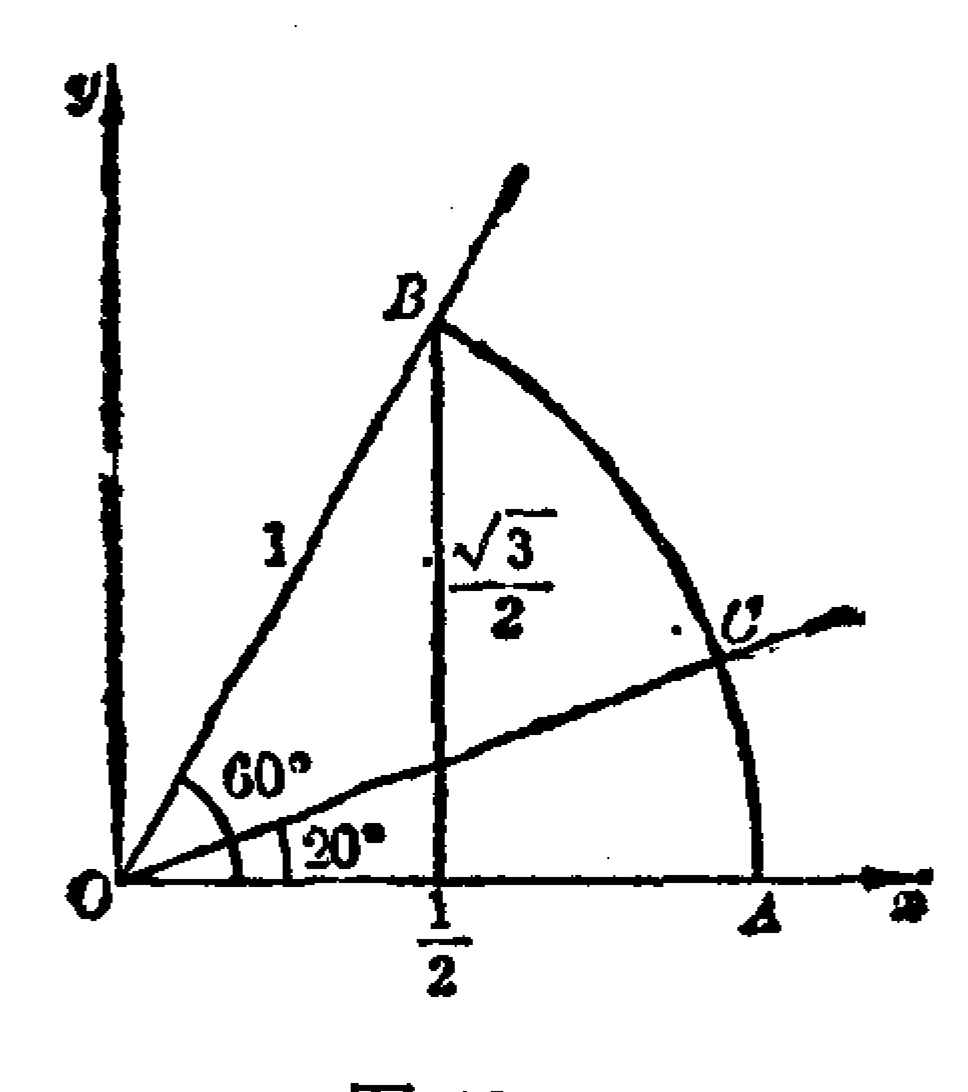


图 10

半径作圆弧，交其一边于 A，另一边于 B，则在直角坐标系 $\{xOy\}$ 中，已知点是

$$O=(0,0),\quad A=(1,0),\quad B=\left(\frac{1}{2},\frac{\sqrt{3}}{2}\right).$$

要作的点是 $C=(\mathrm{Cos}20°,\mathrm{Sin}20°)$。若用数的语言来说，三等分 60° 就是根据三个复数 0，1 和 $\frac{1}{2}+\frac{\sqrt{3}}{2}i$ 作出新数 $\mathrm{Cos}20°+i\mathrm{Sin}20°$。

现在把这个问题一般化。我们约定：说某图形或某数可作，总是指它可从已给的若干个点或数出发，限用圆规直尺经有限步作出。在复平面上任意给定 n 个数 $z_1,z_2,\cdots,z_n$，$n\geqslant 2$，其中 $z_1=0$，$z_2=1$。我们要构造出一个复数集 M，它由全体可作数组成。为此，采用递归方法逐个定义出 W 的如下子集：$S_1,S_2,S_3,\cdots\cdots$。首先定义

$$S_1=\{z_1,z_2,\cdots\cdots,z_n\}.$$

再由 S_1 定义出 S_2，由 S_2 定义出 $S_3,\cdots\cdots$，一般地，如果点集 S_r 已经定义好了，取

$L=\{$连接 S_r 中不同两点的直线$\}$，

$O=\{$任取 $P, Q_1, Q_2 \in S_r$，以 P 为圆心，以 $|Q_1Q_2|$ 为半径所作的圆$\}$，

$\Sigma_1=\{L$ 中任意两条直线的交点$\}$，

$\Sigma_2=\{L$ 中任一直线与 O 中的任一圆的交点$\}$

$\Sigma_3=\{O$ 中任意两个圆的交点$\}$，

则定义

$$S_{r+1}=S_r \cup \Sigma_1 \cup \Sigma_2 \cup \Sigma_3,$$

这里 $\cup$ 表示求集合的并集。最后可以证明

$$M=\bigcup_{i=1}^{\infty} S_i$$

就是所要求的全体可作数集合。事实上，如果某个复数 z 可作，因为圆规仅能据三个已知点作圆，直尺仅能据两个已知点连直线，所以这个 z 必属于某个 S_i，因而 $z\in M$。反之，M 虽然是无限个有限集 S_i 之并，它是一个无限集，但这些 S_i 都是一个包含一个的，所以对于一个取定的 $z\in M$ 来说，必存在某个确定的包含这个 z 的最小的 S_i。根据 S_i 的产生过程知 z 必可作。这就说明了 z 可作当且仅当 $z\in M$。这样一来，问题就转化为考虑复数集 M 的代数结构了。这种演化问题的方法在数学中是经常采用的。

定理 2·1 M 必是复数域 C 的满足下述条件的最小子域：它包含所有的已给数 $z_1, z_2, \cdots\cdots, z_n$，且在开平方和取共轭之下是封闭的，即若 $z\in M$，则 $\sqrt{z}\in M$；若 $z=x+iy\in M$，则 $\bar{z}=x-iy\in M$。

证 证明分以下两步完成。

(1) 首先，$S_1=\{z_1,\cdots\cdots,z_n\}\subset M$。为了证明 M 是 C 的子域，只要证明 M 对加减乘除封闭。任取两个复数 $z=re^{i\theta}=x+iy$，$z'=r'e^{i\theta'}=x'+iy'$，则有以下结论：

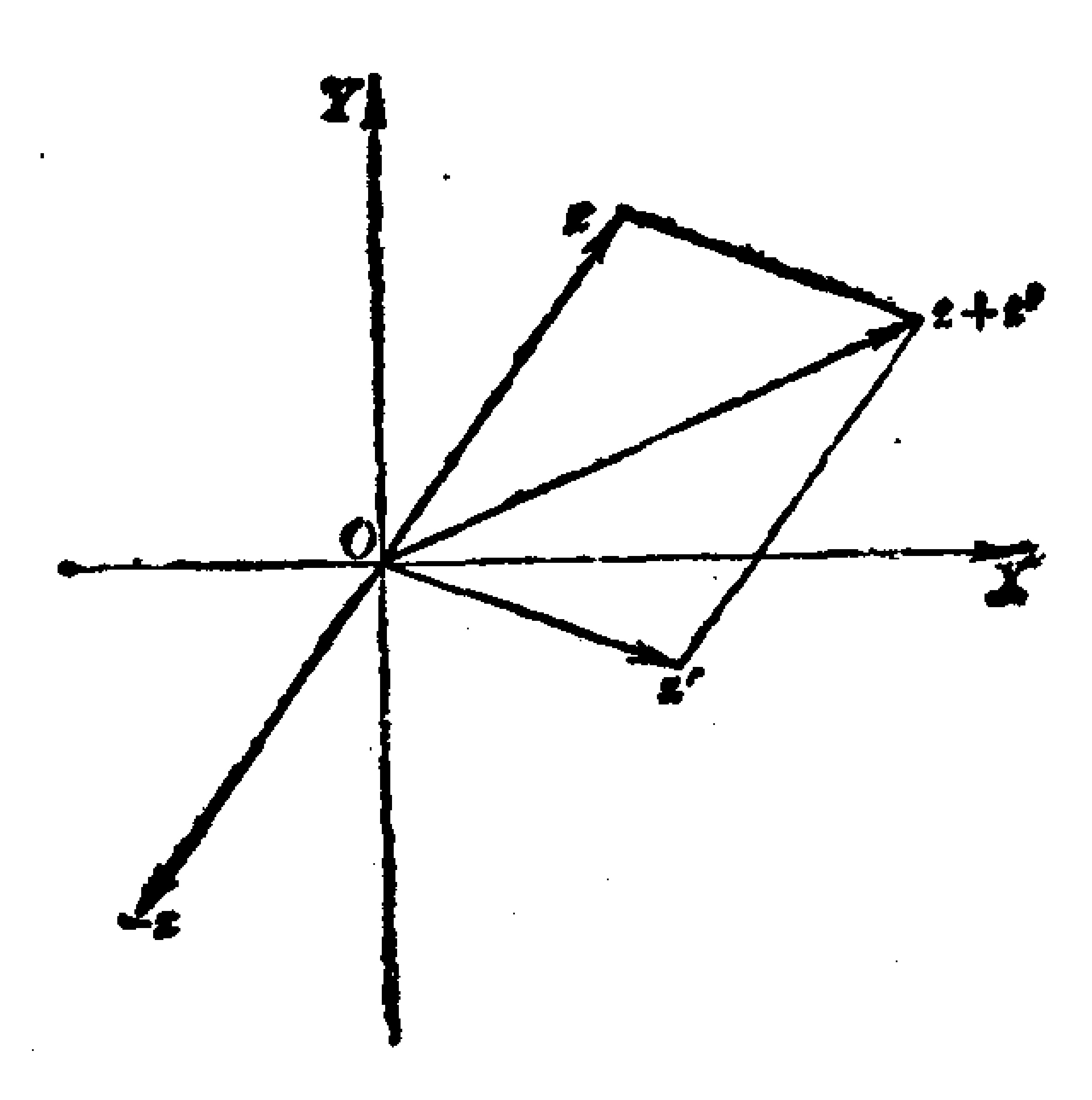


图 11

① 以 z 为圆心，$|z'|$ 为半径作圆 O_1；以 z' 为圆心，$|z|$ 为半径作圆 O_2。由 M 的定义知，两圆的交点 $z+z'\in M$。

② 以原点 o 为圆心，$|z|$ 为半径所作的圆与直线 oz 的另一交点 $-z\in M$，

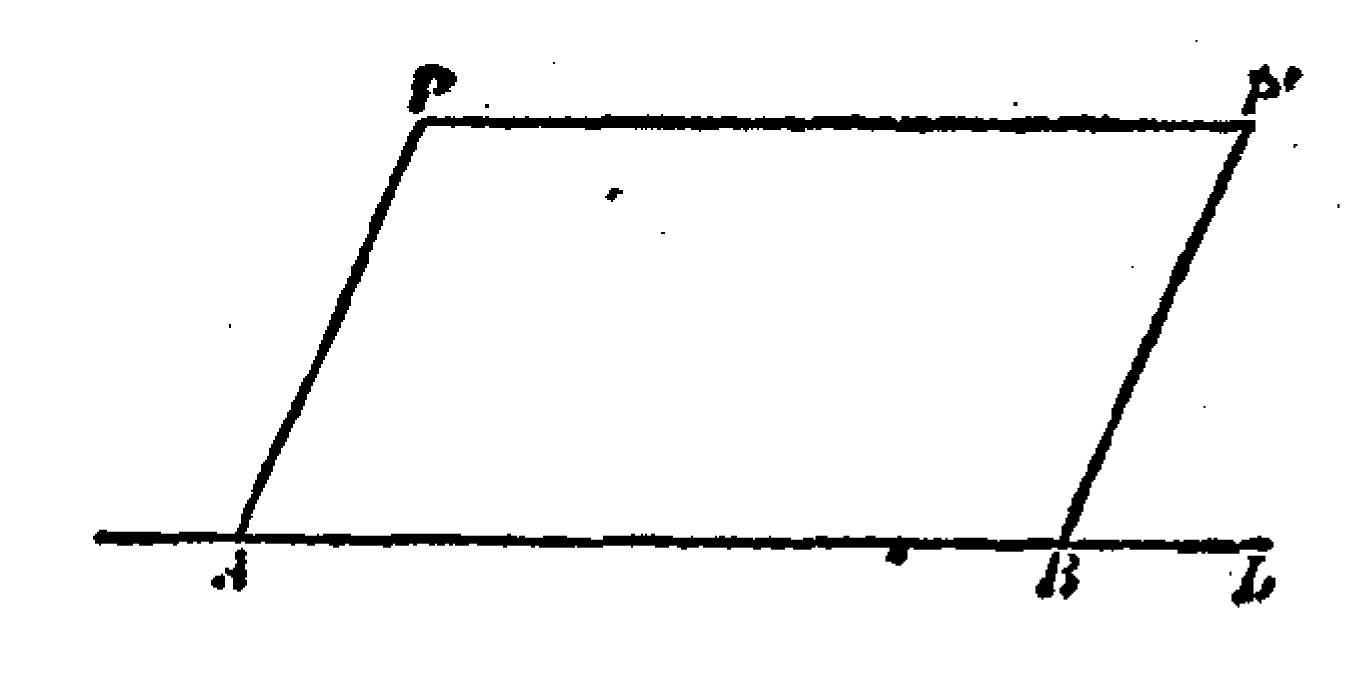


图 12

③ $zz'=rr'e^{i(\theta+\theta')}$。显然，据 θ 和 θ' 必可作出和角

$\theta+\theta'$。另外，总可用圆规直尺过直线 L 外一点 P 作与此直线平行的线。事实上，在 L 上任取两点 A 和 B（见图 12）。连接 PA。以 P 为圆心，$|AB|$ 为半径作圆；以 B 为圆心，$|AP|$ 为半径作圆，两圆交于 P'，则 PP' 即为所求之直线①。据此，在直角坐标系的 x 轴上取 1 和 r 两点，在 y 轴上取 r' 点。连 $r'1$，（见图 13）则易见过 r 所作的 $r'1$ 的平行线必交 y 轴于 rr'，所以 rr' 可作，于是 zz' 可作。

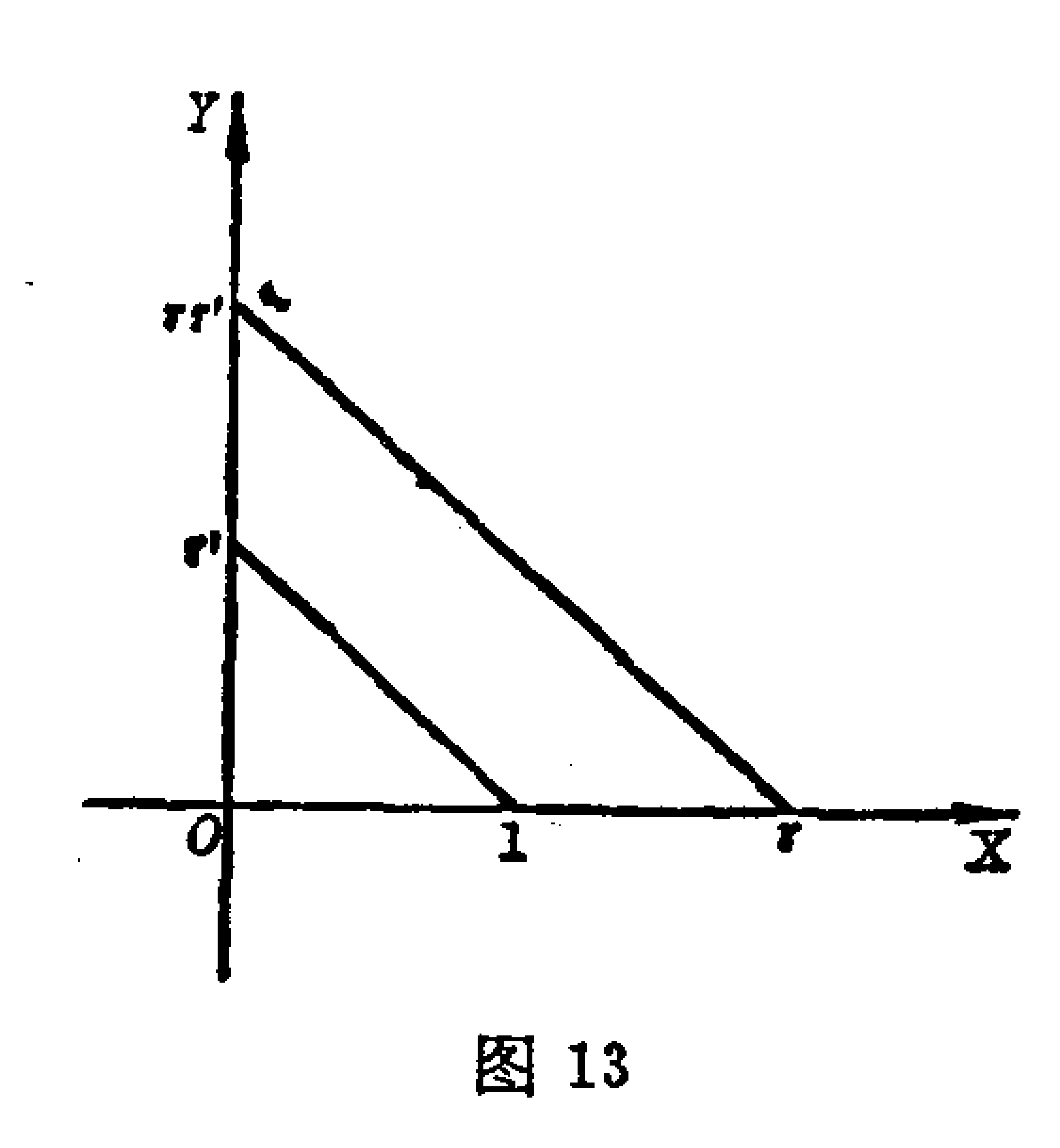


图 13

④ $z^{-1}=(1/r)e^{i(-\theta)}$。由 θ 可作出 $-\theta$。在 x 轴上取 1 和 r 两点，在 y 轴上取点 1，连 $1r$，过 x 轴上的点 1 作 $1r$ 的平行线必交 y 轴于 $1/r$，于是 z^{-1} 可作。

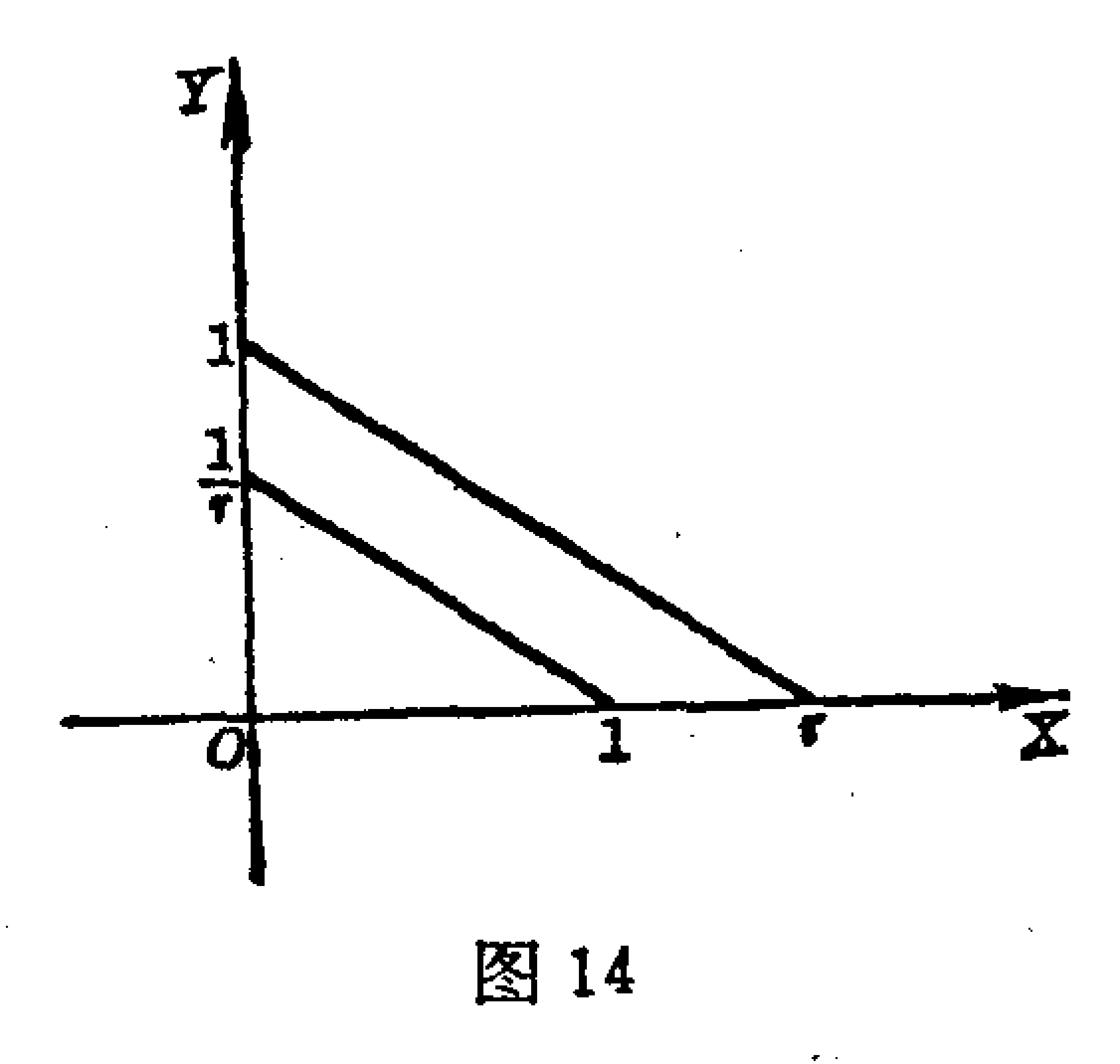


图 14

根据以上 4 点就知 M 是 C 的子域，再证 M 具有两个封闭性。

⑤ $\sqrt{z}=\sqrt{r}e^{i(\theta/2)}$。由 θ 可作出 $\theta/2$。在直角坐标系的 x 轴上取 A 和 B 两点，使 $|OA|=1$，$|AB|=r$。以

---

① 应用推平行线的方法，不难证明用圆规直尺可把任一线段 $\overline{AB}$ 作 n 等分，其中 n 是任一自然数。为此，过 A 点任作直线 L(不与 AB 重合)。在 L 上任意截取 n 个相等的线段 $AC_1=C_1C_2=\cdots C_{n-1}C_n$。连 BC_n，依次过 $C_1, C_2, \cdots, C_{n-1}$ 作 BC_n 的平行线，分别交 AB 于 $B_1, B_2, \cdots, B_{n-1}$，则 $AB_1=AB/n$。

$|OB|$ 为直径作半圆，过 A 作其垂线交半圆于 P，则 $|AP|=\sqrt{r}$。所以当 z 可作时，$\sqrt{z}$ 必可作。

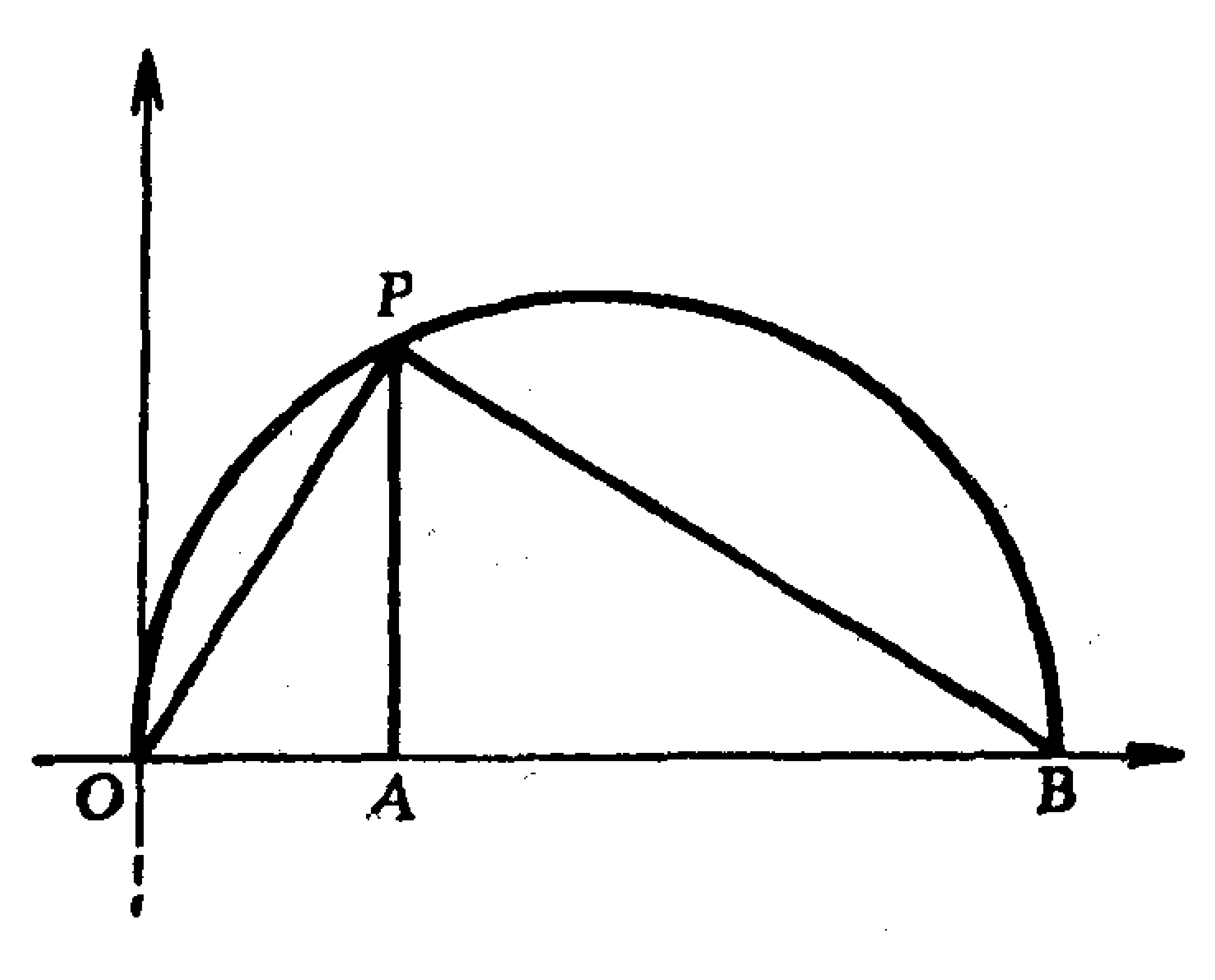


图 15

⑥ $\overline{z}=re^{i(-\theta)}$。由 θ 可作出 $-\theta$，所以若 z 可作，则 $\overline{z}$ 必可作。

这样就证明了 M 是具有上述两个封闭性的域。

(2) 证明 M 具有定理中所说的最小性，即若 M' 是 C 的满足以下条件的某个子域：它包含已给数 $z_1, z_2, \cdots\cdots, z_n$，且在开平方与取共轭之下封闭，要证 $M\subseteq M'$。我们知道，$M=\bigcup\limits_{i=1}^{\infty}S_i$，而 $S_{i+1}=S_i\cup\Sigma_1\cup\Sigma_2\cup\Sigma_3$。由于已知 $S_1=\{z_1, z_2, \cdots, z_n\}\subseteq M'$，很自然地会想到最简单的证明方法是根据 $S_i\subseteq M'$ 证明 $S_{i+1}\subseteq M'$，为此只要证明由 S_i 确定的 Σ_1, Σ_2 和 $\Sigma_3\subset M'$。首先，Σ_1 中的点都是某两条不平行的直线

$$L_1: ax+by+d=0,\quad L_2: a'x+b'y+d'=0$$

的交点。L_1 是 S_i 中某两点 x_1+iy_1，x_2+iy_2 的连线。因为 $x_1+iy_1\in S_i\subseteq M'$，$M'$ 关于共轭封闭，所以 $x_1-iy_1\in M'$，于

是 $x_1 \in M'$. 又据 $-1 \in M'$ 和 M' 关于开平方封闭，知 $i=\sqrt{-1} \in M'$，于是又得 $y_1 \in M'$。同理 $x_2, y_2 \in M'$。而 L_1 的方程就是

$$\frac{x-x_1}{x_2-x_1}=\frac{y-y_1}{y_2-y_1},$$

所以 L_1 的系数 $a, b, d \in M'$。同理，L_2 的系数 $a', b', d' \in M'$。根据求解二元线性方程组的克莱姆法则知，L_1 与 L_2 的交点坐标 p 和 q 都属于 M'。再由 $i \in M'$ 知 $p+iq \in M'$，所以 Σ_1 中的点都属于 M'。其次，Σ_2 中的点都是下述直线和圆的交点：

$$L: y=mx+b, \quad O: x^2+y^2+ex+fy+g=0。$$

L 是 S_i 中某两点的连线，由上所证可知其系数 $m, b \in M'$。圆 O 是以 S_i 中某点 x_0+iy_0 为圆心，以 x_1+iy_1 和 x_2+iy_2 间的长度 $r=\sqrt{(x_1-x_2)^2+(y_1-y_2)^2}$ 为半径所作的圆，其方程为

$$(x-x_0)^2+(y-y_0)^2=r^2。$$

因为所有 x_i, y_i 都属于域 M'，且 M' 关于开平方封闭，所以 $r \in M'$，即圆方程的系数 $e, f, g \in M'$。L 与 O 的交点 (p, q) 中的 p 是二次方程

$$x^2+(mx+b)^2+ex+f(mx+b)+g=0$$

的根，它可用系数的加减乘除和开平方运算表出，而 M' 是关于开平方封闭的域，所以 $p \in M'$，因而 $q=mp+b \in M'$，$p+iq \in M'$。所以 Σ_2 中的点都属于 M'。最后，Σ_3 中点都是以

下两圆的交点：

$$O_1: x^2+y^2+ex+fy+g=0,$$

$$O_2: x^2+y^2+e'x+f'y+g'=0,$$

它就是 O_1 与以下直线（它是这两圆的交点的连线）

$$L: (e-e')x+(f-f')y+g-g'=0$$

的交点。O_1 和 O_2 都是由 S_i 中三点所决定的圆，其系数都属于 M'，因此，由 O_1 与 L 的交点 (p,q) 确定的 $p+iq\in M'$，这样又有 $\Sigma_3\subseteq M'$。这就证明了 $S_{i+1}\subseteq M'$。

我们先来粗略地考察一下，第三章中所说的扩域理论对数的可作性研究有何贡献？给定复数 $z_1,\cdots\cdots,z_n$，也就给定了共轭复数 $\bar{z}_1,\cdots\cdots,\bar{z}_n$。如果已知某数 $z\in M$，则 z 必属于某个 $S_{i+1}=S_i\cup\Sigma_1\cup\Sigma_2\cup\Sigma_3$。根据定理 2.1 的证明过程中对 Σ_1，Σ_2，Σ_3 中那些交点来源所作的分析，可知那些交点坐标 (p,q) 可用 S_i 中的数经过加减乘除、至多再加上一个开平方运算得出。对前四种运算，域并不需要扩大，对开平方运算来说，则需要作一个二次扩域。所以这个数 z 一定在 $F=Q(z_1,\cdots\cdots,z_n,\bar{z}_1,\cdots\cdots,\bar{z}_n)$ 的某个扩域 K 中，而且必有 $[K:F]=2^s$。再据 $F\subseteq F(z)\subseteq K$ 知，$[F(z):F]=2^t$，$t\leqslant s$。于是可得一个重要的结论：可作数 z 必是上述 F 上的 2^t 次代数元。如果读者对这个粗糙的推理感到不满足，则可以读一下如下确切的叙述和严格的证明。

定理 2·2 （判别准则 A）设 $z_1,z_2,\cdots\cdots,z_n$ 是给定的复数。令 $F=Q(z_1,\cdots\cdots,z_n,\bar{z}_1,\cdots\cdots,\bar{z}_n)$，则某数 z 可由 $z_1,z_2,\cdots\cdots,z_n$ 作出 $\Longleftrightarrow$ 存在 C 的某个子域 $K=F(u_1,\cdots\cdots,u_r)$，它包含 z，且 $u_1^2\in F$，$u_i^2\in F(u_1,\cdots\cdots,u_{i-1})$，$i=2,\cdots,r$。

这就是说，K 是包含 z 的 C 的子域，且 K/F 有根次数全是 2 的根塔(平方根塔)：

$$F\subseteq F(u_1)\subseteq F(u_1,u_2)\subseteq\cdots\cdots\subseteq F(u_1,u_2,\cdots\cdots,u_r)=K, \quad (1)$$

证 在 F 上能够建造出很多包含 z 的平方根塔，把所有这种平方根塔中的数放在一起，记为 M'，即

$$M'=\{z|z\in C,\text{存在 } F \text{ 上的某个平方根塔包含 } z\}。$$

因为已知 z 可作$\Longleftrightarrow z\in M$，所以只要证明 $M=M'$ 就行了。

先证 $M'\subseteq M$，即任一被某个平方根塔罩住的 z 必可作。任取 $z\in M'$，则存在平方根塔(1)，且 $z\in K$。因为 $F=Q(z_1,\cdots\cdots,z_n,\ \bar{z}_1,\cdots,\bar{z}_n)$ 中的数都是由有理数和 z_i，$\bar{z}_i$ 作加减乘除而得的，所以 F 中数都可作，$F\subseteq M$。因为 M 关于开平方封闭，由 $u_1^2\in F$ 知 $u_1\in M$，再由 M 是域知 $F(u_1)\subseteq M$。一般地，若已知 $F(u_1\cdots\cdots,u_{i-1})\subseteq M$，则由 $u_i^2\in F(u_1,\cdots\cdots,u_{i-1})$ 知 $u_i\in M$，$F(u_1,\cdots,u_i)\subseteq M$。如此下去，最后证得$K=F(u_1,\cdots\cdots,u_r)\subseteq M$。再由 $z\in K$ 知 $z\in M$，所以 $M'\subseteq M$。再证 $M\subseteq M'$。如果能证明 M' 是 C 的包含 $z_1,\cdots\cdots,z_n$ 的且在共轭与开平方之下封闭的子域，则据定理 2.1 所证明的 M 的那种“最小性”立得 $M\subseteq M'$，于是必有 $M=M'$。现分三步证明 M' 的确是那种子域。

(1) 任取 $z,z'\in M'$，可设

$$z\in F(u_1,\cdots\cdots,u_r)=K,\quad z'\in F(u'_1,\cdots\cdots,u'_s)=K',$$

这里 K 和 K' 都是以 F 为塔基的平方根塔的塔顶。把第二个塔中 s 个添加元依次添加到第一个塔的塔顶 K 上去，得到 $F(u_1,\cdots,u_r,\ u'_1,\cdots,u'_s)$，它在 F 上也有平方根塔：

$$F\subseteq F(u_1)\subseteq\cdots\cdots\subseteq F(u_1,\cdots\cdots,u_r)=K$$
$$\subseteq K(u'_1)\subseteq\cdots\cdots\subseteq K(u'_1,\cdots\cdots,u'_s)$$
$$=F(u_1,\cdots\cdots,u_r,u'_1,\cdots\cdots,u'_s),$$

且包含 $z\pm z'$，zz' 和 $z^{-1}(z\neq 0)$，所以它们都属于 M'。这说明 M' 的确是 C 的包含 $z_1,\cdots,z_n$ 的子域。

(2) 任取 $z\in M'$，设 $z\in F(u_1,\cdots\cdots,u_r)=K$，$K$ 在 F 上有平方根塔。如果 $\sqrt{z}\notin K$，则令 $u_{r+1}=\sqrt{z}$ 就有 $u_{r+1}^2=z\in K$，所以 $K(u_{r+1})$ 在 F 上也有平方根塔且包含 $\sqrt{z}$，于是 $\sqrt{z}\in M'$。

(3) 易见对 $F=Q(z_1,\cdots,z_n,\bar{z}_1,\cdots,\bar{z}_n)$ 有 $\bar{F}=F$，这里 $\bar{F}$ 表示把 F 中所有的数都取共轭数所成的域。因为 $F(u_1,\cdots,u_r)$ 中的数都是 $u_1,\cdots,u_r$ 的有理分式，系数属于 F，所以把其中所有的数都取共轭之后所得的域

$$\overline{F(u_1,\cdots,u_r)}=F(\bar{u}_1,\cdots\cdots,\bar{u}_r)。$$

于是，对任意 $z\in F(u_1,\cdots\cdots,u_r)$，必有 $\bar{z}\in F(\bar{u}_1,\cdots\cdots,\bar{u}_r)$。易见对 $F(u_1,\cdots\cdots,u_r)$ 在 F 上的平方根塔取共轭可得到一个 $F(\bar{u}_1,\cdots\cdots,\bar{u}_r)$ 在 F 上的平方根塔，所以当 $z\in M'$ 时必有 $\bar{z}\in M'$。▌

推论 设 $F=Q(z_1,\cdots\cdots,z_n,\bar{z}_1,\cdots\cdots,\bar{z}_n)$。如果复数 z 可由 $z_1,\cdots\cdots,z_n$ 作出，则 z 必是 F 上的 2^t 次代数元。

证 由 $z\in M$ 知，z 必属于某个域 K，K 在 F 上有平方根塔，所以 $[K:F]=2^s$。再由 $F\subseteq F(z)\subseteq K$ 知 $[F(z):F]=2^t$，$t\leqslant s$，z 是 F 上 2^t 次代数元。▌

由于 F 上任一 2^t 次代数元 z 未必有一个平方根塔罩住它，所以这种 z 未必可作。这说明上述推论仅提供了 z 可作

的必要条件。但这对于要证明"不可作性"来说刚好是正中下怀！不满足必要条件的数一定不可作。据此，我们一举就可解决如下三个几何难题。

1．三等分任意角。 取 $P_1=(0,0)$，$P_2=(1,0)$，$P_3=\left(\frac{1}{2},\frac{1}{2}\sqrt{3}\right)$，则

$\alpha=60^\circ$ 能用圆规直尺三等分

$\Longleftrightarrow P=(\text{Cos}20^\circ,\text{Sin}20^\circ)$ 可作

$\Longleftrightarrow a=\text{Cos}20^\circ$ 可作

$\Longleftrightarrow a$ 是 F 上 2^t 次代数元，这里

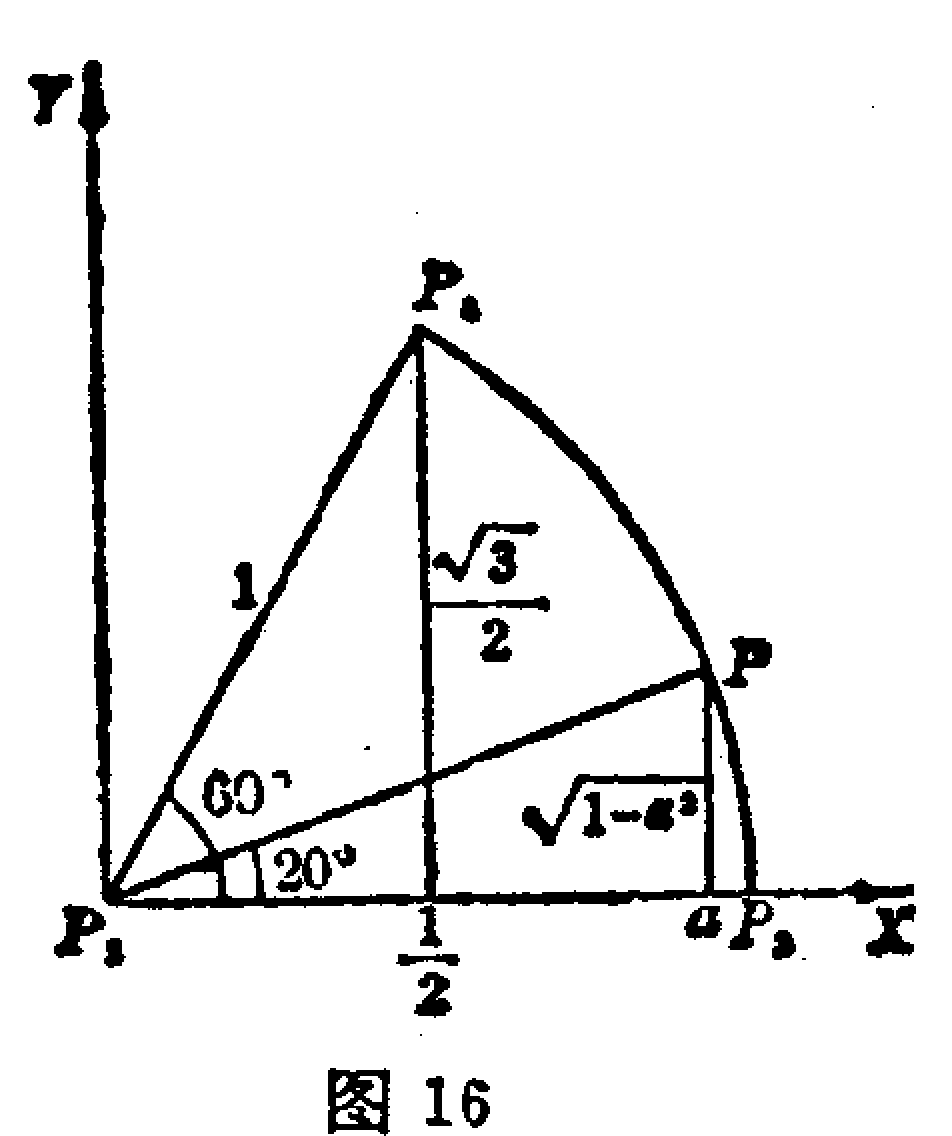


图 16

$$F=Q\left(0,1,\frac{1}{2}+\frac{\sqrt{3}}{2}i,\frac{1}{2}-\frac{\sqrt{3}}{2}i\right)=Q(\sqrt{3}i),$$

它是 Q 的 2 次扩域。如果 a 是 F 上 2^t 次代数元，则必是 Q 上 2^{t+1} 次代数元，即 a 在 Q 上的最小多项式的次数应是 2^{t+1}。但是可以证明，这是决不可能的。事实上，在

$$\text{Cos}\,3\theta=4\,\text{Cos}^3\theta-3\,\text{Cos}\,\theta$$

中取 $\theta=20^\circ$，$a=\text{Cos}\,20^\circ$，就有

$$4a^3-3a=\text{Cos}\,60^\circ=\frac{1}{2},$$

即 $(2a)^3-3\cdot(2a)-1=0$。但 x^3-3x-1 显然是 $Q[x]$ 中 3 次不可约多项式，$2a$ 是 Q 上 3 次代数元，所以 $2a$ 不可作，即 a 不可作，因此 60° 不能用圆规直尺三等分。

关于"三等分角问题"的确切结论是：的确存在不能限用圆规直尺经有限步实现三等分的角。另一方面，又确实存在

一大批可以三等分的角。例如，可证只要 n 不是 3 的倍数，则 $a=\pi/n$ 必可三等分。事实上，此时 n 和 3 必是互素的，必存在整数 u 和 v 使 $3u+nv=1$，$1/3n=u/n+v/3$，所以

$$\frac{1}{3}a=\frac{1}{3n}\pi=u\frac{\pi}{n}+v\frac{\pi}{3}=ua+v60^\circ.$$

由圆内接正六边形可作知 60° 可作，可作角 a 的倍数必可作，所以 $a/3$ 可作。

2. **倍立方.** 设原立方体的棱长为 1，则求倍立方体的棱长相当于作出 $x^3-2=0$ 的根 $z=\sqrt[3]{2}$。现在 $F=Q(2)=Q$，而 z 是 Q 上 3 次代数元，所以 $\sqrt[3]{2}$ 也不可作。

3. **化圆为方.** 设圆的半径为 1，则求正方形的边长相当于作出 $x^2-\pi=0$ 的根 $z=\sqrt{\pi}$。但 π 不是 Q 上的代数元，所以必不可作。

这三个难题解决了，接下去要考虑哪些正 n 边形可作。读者可能已经看出，应用上述判别准则 A 的充分条件是很不方便的，现在我们把它改造一下。

定理 2·3 （判别准则 B）设 $z_1,z_2,\cdots,z_n$ 是给定的复数。令 $F=Q(z_1,\cdots,z_n,\ \bar{z}_1,\cdots,\bar{z}_n)$，则某数 z 可由 $z_1,\cdots,z_n$ 作出 $\Longleftrightarrow$ z 是 F 上代数元，且 $F(z)/F$ 的正规闭包 K/F 的次数 $[K:F]=2^t$，t 是某个非负整数。

证 必要性。设 z 可作，由判别准则 A 知，存在 F 的扩域 L 使 $z\in L$ 且 L/F 有平方根塔，则 L/F 的正规闭包 $\widetilde{L}/F$ 也有平方根塔，（见第 129 页）可设 $[\widetilde{L}:F]=2^s$。由 $z\in L$ 得

$$F\subseteq F(z)\subseteq L\subseteq \widetilde{L},$$

且 $\widetilde{L}$ 是 F 的包含 $F(z)$ 的正规扩域。但由假设知，K 是 $F(z)/F$ 的正规闭包，所以 K 是 F 的包含 $F(z)$ 的最小正规扩域（见

第 97 页)，所以必有

$$F\subseteq K\subseteq \widetilde{L},$$

于是 $[K:F]=2^t$，$t\leqslant s$。

充分性：设 $[K:F]=2^t$。因为 K/F 是伽罗瓦扩域，记 $G=\mathrm{Gal}\,K/F$，必有 $|G|=[K:F]=2^t$。对于这种 G 必有极大正规子群 G_2，且 $|G_2|=2^{t-1}$(证明略)。同理，G_2 也有极大正规子群 G_3，$|G_3|=2^{t-2}$……如此下去，可得 G 的合成群列

$$G=G_1\rhd G_2\rhd G_3\rhd\cdots\cdots\rhd G_t\rhd G_{t+1}=1,$$

且 $|G_i/G_{i+1}|=2$，$i=1,2,\cdots\cdots,t$。在伽罗瓦对应之下有

$$F=F_1\subset F_2\subset F_3\subset\cdots\cdots\subset F_t\subset F_{t+1}=K,$$

其中 $[F_{i+1}:F_i]=2$，$i=1,2,\cdots\cdots,t$。这说明 F_{i+1} 必是 F_i 的 2 次单代数扩域，$F_{i+1}=F_i(u_i)$，其中 u_i 满足二次方程

$$u_i^2+a_iu_i+b_i=0,\quad a_i,b_i\in F_i.$$

但它可改写成

$$\left(u_i+\frac{1}{2}a_i\right)^2=\frac{1}{4}a_i^2-b_i.$$

令 $v_i=u_i+a_i/2$，$b_i'=a_i^2/4-b_i$，有 $v_i^2=b_i'\in F_i$，且

$$F_{i+1}=F_i(v_i)。$$

这说明 F_{i+1} 是 F_i 的平方根号扩域 $(i=1,2,\cdots\cdots,t)$。因此 K/F 有平方根塔，且 $z\in K$，于是由判别准则 A 知 z 可由 z_1，……，z_n 作出。▌

运用这个判别准则可以彻底解决正 n 边形作图问题。

我们首先指出：若 s 是某个自然数使得 2^s+1 是素数，

则必存在非负整数 t 使 $s=2^t$。事实上，如果 s 有奇数真因子 u 使 $s=uv$，则由

$$2^s+1=(2^v+1)(2^{(u-1)v}-2^{(u-2)v}+2^{(u-3)v}-\cdots+1)$$

知 2^s+1 不是素数。凡形如 $2^{2^t}+1$ 的素数称为**费马素数**。最小的 5 个费马素数是

$$3,\ 5,\ 17,\ 257,\ 65537,$$

分别对应 $t=0,1,2,3,4$。费马（P·Fermat，1601～1665）出身于法国的一个皮革商家庭，一生中大部分时间里以律师为职业'数学仅是他的业余爱好。他有很了不起的直观天才，一生中作出了很多猜测，并有不少数学成果。他发表的论文很少，大多数成果是通过他给别人的信件才流传于世的。他有时还把自己的研究心得写在书页的空白处。令人钦佩的是，费马所作的猜测几乎全被证实了，但有两个例外。一个就是被称之为费马大定理的猜测：对 $n\geqslant3$，$x^n+y^n=z^n$ 不存在整数解，它已成为世界上悬赏最高的难题，但至今仍未获解决。另一个猜测是：任一形如 $2^{2^t}+1$ 的数必是素数，关于这件事他却猜错了！1738 年，欧拉证明，当 $t=5$ 时，

$$2^{2^5}+1=4294967297=641\times6700417,$$

因此它不是素数！有趣的是，到目前为止，人们再也没有找到第六个形如 $2^{2^t}+1$ 的数是素数，相反地，倒已经证明了 46 个这种数不是素数。因此，又有人猜测：费马素数仅有上述 5 个，当然，这一点目前也没有得到证明。

好了，言归正传，让我们继续讨论正多边形的构作问题。任意取定某个自然数 n，ω 是 n 次本原根，则前已提到，$Q(\omega)/Q$ 是 $\varphi(n)$ 次伽罗瓦扩域（见第 92 页）。由判别准则 B 知

正 n 边形可作 $\Longleftrightarrow \omega$ 可作 $\Longleftrightarrow \varphi(n)$ 是 2 的方幂。

设 $n=2^e p_1^{e_1} p_2^{e_2} \cdots\cdots p_s^{e_s}$，$p_i$ 为两两不同的奇素数。如果 $n=2^e$，$e\geqslant 1$，显然，正 2^e 边形必可作。因此仅需讨论 $e\geqslant 0$ 且所有 $e_i\geqslant 1$ 的情形。对于任一素数的方幂 p^k，必有 p^{k-1} 个不超过 p^k 的自然数与 p^k 不互素，所以根据欧拉函数的定义，知

$$\varphi(p^k)=p^k-p^{k-1}=p^{k-1}(p-1)。$$

再利用循环群的性质可以证明：当 r 与 s 互素时，必有 $\varphi(rs)=\varphi(r)\varphi(s)$，所以得到

$$\varphi(n)=\varphi(2^e)\cdot\varphi(p_1^{e_1})\cdot\varphi(p_2^{e_2})\cdots\cdots\varphi(p_s^{e_s})$$

$$=\begin{cases} 2^{e-1}p_1^{e_1-1}(p_1-1)\cdot p_2^{e_2-1}(p_2-1)\cdots\cdots p_s^{e_s-1}(p_s-1), \\ \quad 若\ e\geqslant 1, \\ p_1^{e_1-1}(p_1-1)\cdot p_2^{e_2-1}(p_2-1)\cdots\cdots p_s^{e_s-1}(p_s-1), \\ \quad 若\ e=0。\end{cases}$$

易见 $\varphi(n)$ 是 2 的方幂 $\Longleftrightarrow$ 所有 $e_i=1$ 且 $p_i=2^{k_i}+1$，于是得到

定理 2·4　正 n 边形可作 $\Longleftrightarrow n=2^e p_1 p_2 \cdots\cdots p_s$，这里 $e\geqslant 0$，$p_1, p_2, \cdots\cdots, p_s$ 是两两不同的费马素数。

据此不难得知，在边数不超过十的正多边形中仅有正七边形和正九边形不可作。因为 3 和 5 都是费马素数，所以边数为

$$3,\ 5,\ 15,\ 2^n,\ 2^n\cdot 3,\ 2^n\cdot 5,\ 2^n\cdot 15,$$

的正多边形必可作，n 是任意自然数。17 是第 3 个费马素数，正十七边形当然可作。可是，理论上证明可作和实际把它作出，这两者之间并不能划等号，往往需要付出极大的智慧和

努力。

作为本书的结束，我们给出边数为 5，15 和 17 的正多边形的作法。

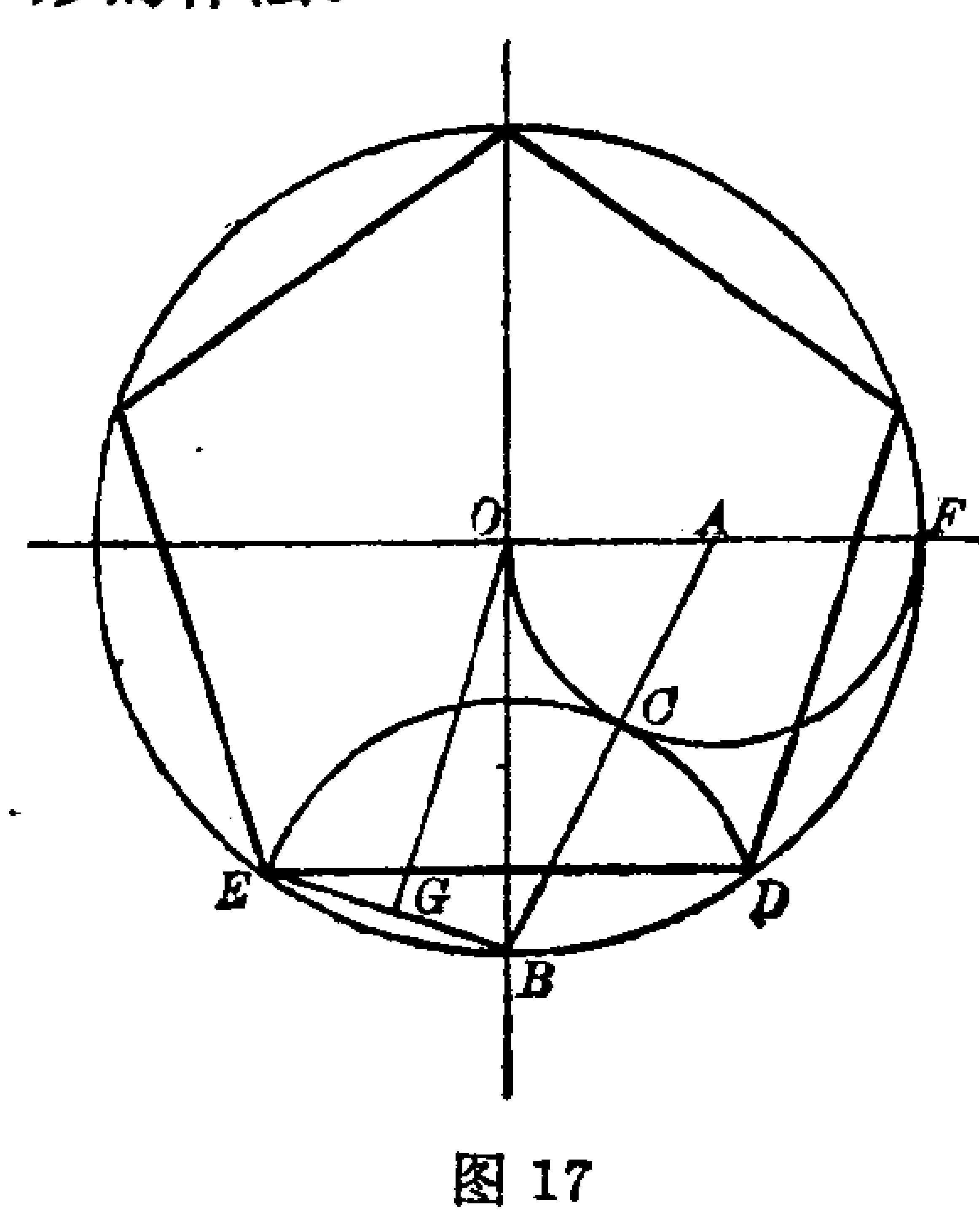


图 17

(1) 正五边形作法。在单位圆O中作两条互相垂直的直径，其端点分别为F和B。(如图)。取半径OF的中点A，连接AB。以A为圆心，1/2OF为半径作半圆，交AB于C。以B为圆心，$|BC|$为半径作圆弧交大圆于E和D两点，则可证ED就是正五边形的边长。事实上，

$$|AB|=\sqrt{|OA|^2+|OB|^2}=\sqrt{1+\frac{1}{4}}=\frac{1}{2}\sqrt{5}.$$

$$|BC|=|AB|-|AC|=\frac{1}{2}(\sqrt{5}-1)=|BE|.$$

作OG垂直BE，交BE于G，因为已知$\sin 18^\circ=\frac{1}{4}(\sqrt{5}-1)$ (见第 123 页)，所以

$$|BE|=2\sin 18^\circ,\quad |BG|=\sin 18^\circ.$$

这说明$\angle BOG=18^\circ$，BE恰好是正十边形的边长。于是证得ED是正五边形的边长。正五边形可作，正$2^n\cdot 5$边形当然都可作了，$n=0,1,2,\cdots\cdots$。

(2) 正十五边形作法。以 A 为一个公共顶点作正三角形 ABC 和正五边形 $APQRS$，则

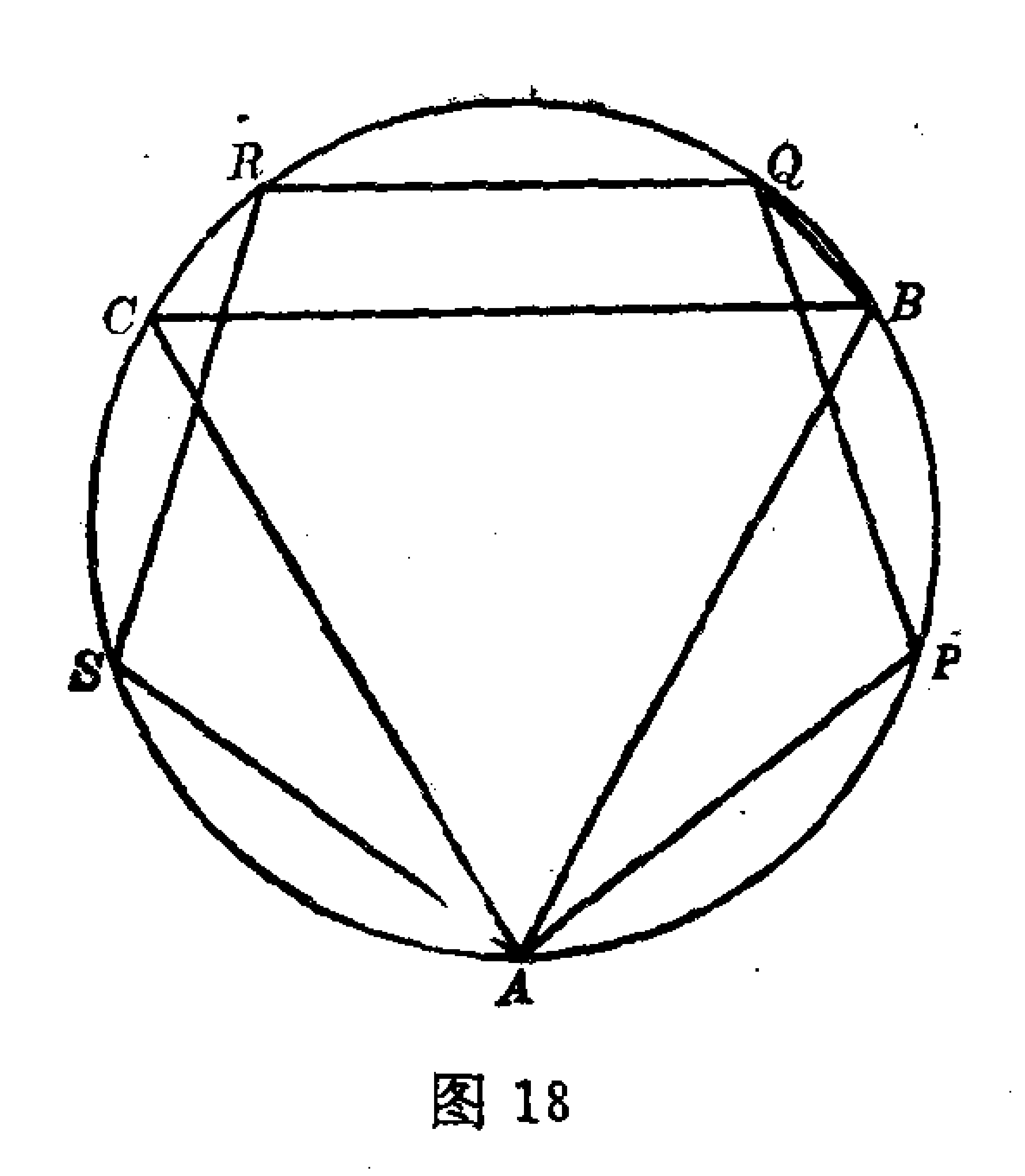


图 18

$$\widehat{BQ}=\widehat{APBQ}-\widehat{APB}$$

$$=\left(\frac{2}{5}-\frac{1}{3}\right)\text{圆周}$$

$$=\frac{1}{15}\text{圆周}。$$

所以 $|BQ|$ 恰好是正十五边形的边长。于是正 $2^n\cdot 15$ 边形都可作。

(3) 正十七边形作法。这要比上述两个作法困难得多了。我们先要推导出作法的依据。令 $\theta=2\pi/17$，$z=\mathrm{Cos}\,\theta+\sqrt{-1}\,\mathrm{Sin}\,\theta$，则

$$z^k=\mathrm{Cos}\,k\theta+\sqrt{-1}\,\mathrm{Sin}\,k\theta,\quad 1\leqslant k\leqslant 17$$

是 17 个 17 次单位根，由

$$x^{17}-1=(x-1)(x^{16}+x^{15}+\cdots\cdots+x+1)$$

和 z^k，$k=1,2,\cdots\cdots,16$，是 17 次本原根全体可知 z 在 Q 上的最小多项式为

$$g(x)=\sum_{i=1}^{16}x^i=\prod_{k=1}^{16}(x-z^k),$$

$g(x)$ 在 Q 上的分裂域是 $E=Q(z)$，$[E:Q]=16$，且

$$G=\mathrm{Gal}\,E/Q=\langle\sigma\rangle$$

为 16 阶循环群，这里

$$\sigma: z \to z^k,\quad \sigma \text{ 不变 } Q \text{ 中数},\quad (k,16)=1。$$

为讨论简单起见，可取 $k=3$，即 $z^\sigma=z^3$。设

$$3^i=17q_i+e_i,\quad 1\leqslant e_i\leqslant 16,\quad i=1,2,\cdots\cdots,16,$$

利用 $z^{\sigma^i}=z^{3^i}$ 和 $z^{17}=1$ 可列出下表

i	1	2	3	4	5	6	7	8
e_i	3	9	10	13	5	15	11	16

i	9	10	11	12	13	14	15	16
e_i	14	8	7	4	12	2	6	1

易见 $G=\langle\sigma\rangle$ 有合成群列

$$G=G_1=\langle\sigma\rangle \rhd G_2=\langle\sigma^2\rangle \rhd G_3=\langle\sigma^4\rangle$$
$$\rhd G_4=\langle\sigma^8\rangle \rhd G_5=1,$$

其中 G_i/G_{i+1} 都是 2 阶群。根据伽罗瓦对应可得平方根塔

$$Q=F_1\subset F_2\subset F_3\subset F_4\subset F_5=E,$$

这里 $F_i=\mathrm{Inv}\,G_i$，$[F_{i+1}:F_i]=2$。现要依次定出 F_{i+1}/F_i 的添加元，$i=1,2,3$。

① 取

$$x_1=\sum_{i=0}^{7} z^{\sigma^{2i}}=\sum_{i=0}^{7} z^{3^{2i}},$$

$$x_2=x_1^\sigma=\sum_{i=0}^{7} z^{\sigma^{2i+1}}=\sum_{i=0}^{7} z^{3^{2i+1}}.$$

由上表可知 $x_1 \neq x_2$，但却有（利用 $z^{3^{16}}=z^{\sigma^{16}}=z$）

$$x_1^{\sigma^2}=\sum_{i=0}^{7} z^{\sigma^{2(i+1)}}=x_1,$$

所以 $x_1 \notin F_1$，但 $x_1 \in F_2=\mathrm{Inv}\langle\sigma^2\rangle$，且 $[F_2:F_1]=2$，所以

$$F_2=F_1(x_1)。$$

② 取

$$y_1=\sum_{i=0}^{3} z^{\sigma^{4i}}=\sum_{i=0}^{3} z^{3^{4i}},$$

$$y_2=y_1^{\sigma^2}=\sum_{i=0}^{3} z^{\sigma^{4i+2}}=\sum_{i=0}^{3} z^{3^{4i+2}}。$$

也有 $y_1 \neq y_2$。由

$$y_1^{\sigma^4}=\sum_{i=0}^{3} z^{\sigma^{4(i+1)}}=y_1$$

知 $y_1 \notin F_2$，$y_1 \in F_3=\mathrm{Inv}\langle\sigma^4\rangle$，必有

$$F_3=F_2(y_1)=F_1(x_1,y_1)$$

③ 取

$$z_1=z+z^{3^8}, \quad z_2=z_1^{\sigma^4}=z^{3^4}+z^{3^{12}}。$$

必有 $z_1 \neq z_2$。由 $z_1^{\sigma^8}=z^{3^8}+z=z_1$ 知 $z_1 \notin F_3$，$z_1 \in F_4=\mathrm{Inv}\langle\sigma^8\rangle$，必有

$$F_4=F_3(z_1)=F_1(x_1,y_1,z_1)。$$

现在可具体求出这些添加元了。由 $g(z)=0$ 知

$$\sum_{k=1}^{16} z^k=-1。$$

再由 $z^k=\mathrm{Cos}\,k\theta+\sqrt{-1}\,\mathrm{Sin}\,k\theta$ 和 $\bar{z}=z^{-1}$ 知

$$z^k+z^{-k}=z^k+\bar{z}^k=2\,\mathrm{Cos}\,k\theta,\quad 1\leqslant k\leqslant 17,$$

于是利用上表可算出

$$x_1=(z+z^{3^8})+(z^{3^2}+z^{3^{10}})+(z^{3^4}+z^{3^{12}})+(z^{3^6}+z^{3^{14}})$$

$$=(z+z^{-1})(z^{-8}+z^8)+(z^{-4}+z^4)+(z^{-2}+z^2)$$

$$=2(\mathrm{Cos}\,\theta+\mathrm{Cos}\,2\theta+\mathrm{Cos}\,4\theta+\mathrm{Cos}\,8\theta),$$

$$x_2=2(\mathrm{Cos}\,3\theta+\mathrm{Cos}\,5\theta+\mathrm{Cos}\,6\theta+\mathrm{Cos}\,7\theta)$$

再利用(1)式知 $x_1+x_2=-1$，经过计算得 $x_1\cdot x_2=4(x_1+x_2)$ $=-4$，于是解得

$$x_1=\frac{1}{2}(\sqrt{17}-1),\qquad x_2=\frac{1}{2}(-\sqrt{17}-1).$$

类似地可算得

$$y_1=2(\mathrm{Cos}\,\theta+\mathrm{Cos}\,4\theta),\qquad y_2=2(\mathrm{Cos}\,2\theta+\mathrm{Cos}\,8\theta).$$

再令

$$y_3=2(\mathrm{Cos}\,3\theta+\mathrm{Cos}\,5\theta),\qquad y_4=2(\mathrm{Cos}\,6\theta+\mathrm{Cos}\,7\theta),$$

则可算出

$$y_1y_2=y_3y_4=x_1+x_2=-1,$$

$$y_1+y_2=x_1,\quad y_3+y_4=x_2.$$

于是可分别解得

$$y_1=\frac{1}{2}(x_1+\sqrt{x_1^2+4})=\frac{1}{4}(\sqrt{17}-1)+\frac{1}{4}\sqrt{34-2\sqrt{17}},$$

$$y_2=\frac{1}{2}(x_1-\sqrt{x_1^2+4}),$$

$$y_3=\frac{1}{2}(x_1+\sqrt{x_2^2+4})=\frac{1}{4}(-\sqrt{17}-1)+\frac{1}{4}\sqrt{34+2\sqrt{17}},$$

$$y_4=\frac{1}{2}(x_2-\sqrt{x_2^2+4})。$$

易见 $z_1=2\,\mathrm{Cos}\,\theta$，$z_2=2\,\mathrm{Cos}\,4\theta$，则由 $z_1+z_2=y_1$，$z_1z_2=y_3$ 解得

$$z_1=\frac{1}{2}(y_1+\sqrt{y_1^2-4y_3}),$$

$$z_2=\frac{1}{2}(y_1-\sqrt{y_1^2-4y_3})。$$

最后可得 $\mathrm{Cos}\,\theta=\frac{1}{2}z_1$，$\mathrm{Sin}\,\theta=\sqrt{1-\mathrm{Cos}^2\theta}$，于是 $z=\mathrm{Cos}\,\theta+\sqrt{-1}\,\mathrm{Sin}\,\theta$ 可作，即正十七边形可作，于是正 $2^n\cdot17$ 边形也可作了。

现在给出具体的作图步骤。作直角坐标系 $\{xoy\}$。(见图 19)。在 x 轴上以 $OA=4$ 为半径作圆 O 交 y 轴于 C。取 $OE=|OA|/4=1$，连结 CE。作

$$EF=EF'=EC=\sqrt{OC^2+OE^2}=\sqrt{17}。$$

在 x 轴上取

$$FG=FC=\sqrt{OC^2+OF^2}=\sqrt{16+(1+\sqrt{17})^2}$$

$$=\sqrt{34+2\sqrt{17}}$$

$$F'G'=F'C=\sqrt{OC^2+OF'^2}=\sqrt{16+(\sqrt{17}-1)^2}$$

$$=\sqrt{34-2\sqrt{17}}$$

以 AG 为直径作圆 O'，与 y 轴交于 H，连结 HG 和 HA 作

$$IH=IJ=\frac{1}{2}OG'=\frac{1}{2}(OF'+F'G')$$

$$=\frac{1}{2}(\sqrt{34-2\sqrt{17}}+\sqrt{17}-1)=2y_1.$$

作 OJ 的中垂线分别交圆 O 于 K 和 L 两点，则可证

$$\angle AOK=2\pi/17,$$

于是 AK 就是所求的正十七边形的边长。事实上，

$$OG=FG-FO=\sqrt{34+2\sqrt{17}}-\sqrt{17}-1=4y_3,$$

$$OH^2=OG\cdot OA=4y_3\cdot 4=16y_3,$$

$$OI=\sqrt{IH^2-OH^2}=\sqrt{4y_1^2-16y_3}=2\sqrt{y_1^2-4y_3},$$

$$OJ=OI+IJ=2y_1+2\sqrt{y_1^2-4y_3}=4z_1,$$

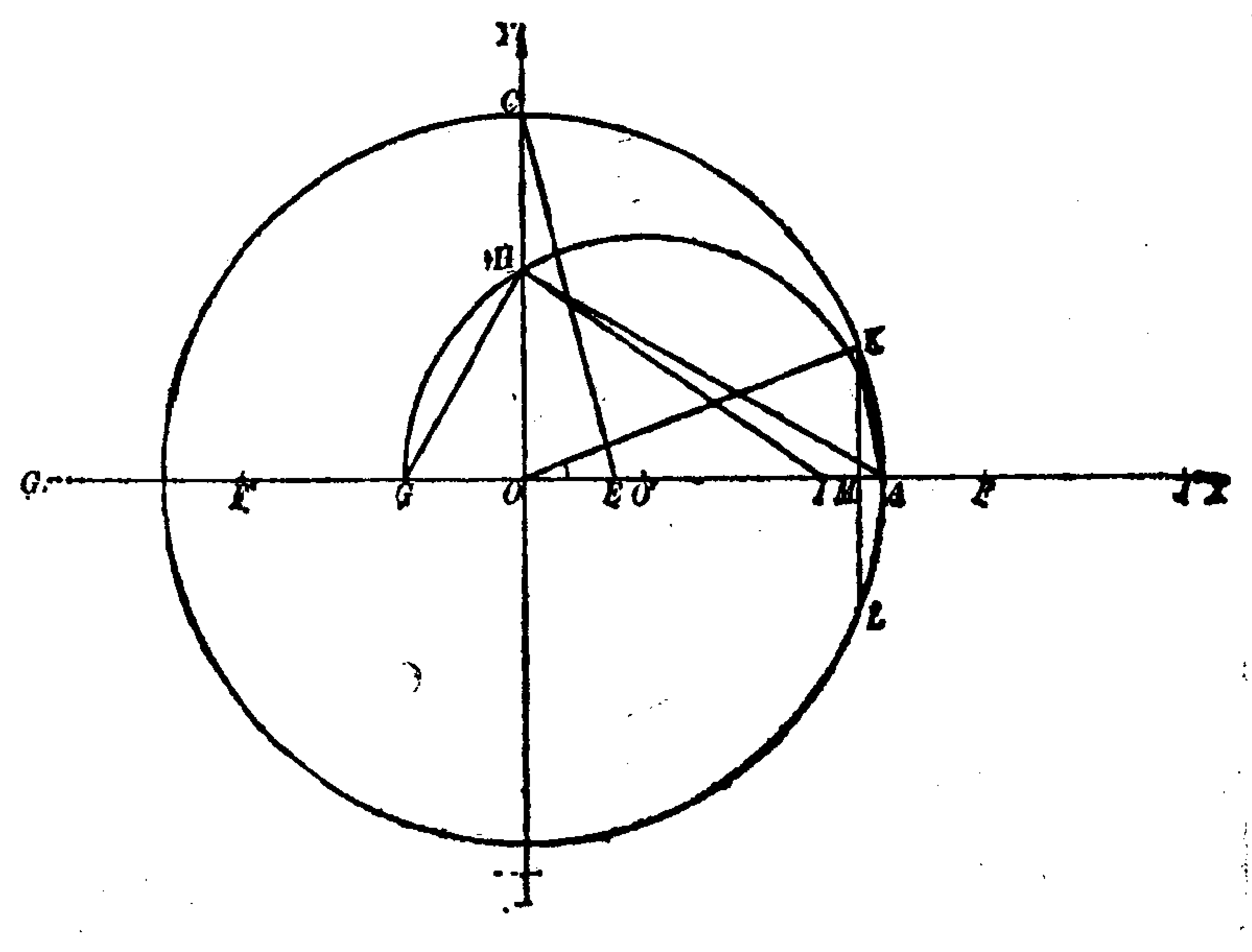


图 19

$$OM=\frac{1}{2}OJ=2z_1,$$

所以 $\cos\angle AOK=\frac{OM}{OK}=\frac{2}{4}z_1=\frac{1}{2}z_1$，$\angle AOK=\frac{2\pi}{17}$。于是正十七边形终于作出来了！

继高斯之后，数学家力西罗给出了正257边形的完善作法，作图过程印出来长达80页。接着盖尔美斯又给出了正65537边形的作法，其手稿就装满了一个手提箱，现保存在德国哥廷根大学。这也许是圆规直尺作图史上的一个最高记录吧。事情已经发展到这一地步，恐怕再也无人愿意去打破这个记录了。

[General Information]
书名=古典数学难题与伽罗瓦理论
作者=徐诚浩
页数=155
SS号=10068318
出版日期=1986年08月第1版